#3

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２０００年　６月　１日

出願番号
Application Number: 特願２０００－１６４８１９

出願人
Applicant(s): 株式会社アズジェント

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年　５月１８日

特許庁長官
Commissioner,
Japan Patent Office 及川耕造

出証番号　出証特２００１－３０４１８４４

【書類名】　特許願
【整理番号】　ASG-0001
【提出日】　平成12年 6月 1日
【あて先】　特許庁長官殿
【国際特許分類】　G09C　5/00
【発明者】
　【住所又は居所】　東京都中央区日本橋小網町１９番７号　株式会社アズジェント内
　【氏名】　杉本　▲隆▼洋
【特許出願人】
　【住所又は居所】　東京都中央区日本橋小網町１９番７号
　【氏名又は名称】　株式会社アズジェント
【代理人】
　【識別番号】　100109014
　【弁理士】
　【氏名又は名称】　伊藤　充
　【電話番号】　03-5366-2677
【手数料の表示】
　【予納台帳番号】　067081
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　セキュリティポリシー構築方法及びセキュリティポリシー構築を支援する装置

【特許請求の範囲】

【請求項１】　所定の団体のセキュリティポリシーを構築する方法において、

セキュリティポリシーのドラフトを構築するドラフト構築ステップと、

前記セキュリティポリシーのドラフトと、団体の実態との差異を調査する分析ステップと、

前記差異に基づき前記セキュリティポリシーのドラフトの調整、または、前記差異に基づき前記団体の実際の情報システムの運用ルールの調整、を行う調整ステップと、

を含むことを特徴とするセキュリティポリシー構築方法。

【請求項２】　請求項１記載のセキュリティポリシー構築方法において、

前記ドラフト構築ステップは、

団体に属するメンバーにするべき質問を生成する生成ステップと、

生成した前記質問を前記メンバーに聞く質問ステップと、

前記質問に対する前記メンバーの回答を取得する回答取得ステップと、

前記取得した回答に基づき、セキュリティポリシーのドラフトを構築する構築ステップと、

を含むことを特徴とするセキュリティポリシー構築方法。

【請求項３】　請求項２記載のセキュリティポリシー構築方法において、

前記生成ステップは、被質問者の職務内容に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項４】　請求項２記載のセキュリティポリシー構築方法において、

前記回答取得ステップは、

前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管するステップと、

前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行

し、矛盾点を解決し、前記記憶手段中に前記回答群を格納するステップと、

前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を決定し、前記記憶手段中に回答群を格納するステップと、

の少なくとも１のステップを含むことを特徴とするセキュリティポリシー構築方法。

【請求項５】　請求項２記載のセキュリティポリシー構築方法において、

前記分析ステップは、

前記取得した回答群中に矛盾する回答が含まれているか否かを検査する矛盾検査ステップと、

前記回答群によって仮想的に想定される情報システムと、前記セキュリティポリシーと、の比較をし差異を検査する第１差異検出ステップと、

前記回答群によって仮想的に想定される情報システムを実際の情報システムの調査でプルーフし、このプルーフした情報システムと、前記セキュリティポリシーのドラフトと、を比較をし差異を検査する第２差異検出ステップと、

の少なくとも１のステップを含むことを特徴とするセキュリティポリシー構築方法。

【請求項６】　請求項５記載のセキュリティポリシー構築方法において、

前記調査した差異の対策をその優先度と共に立てる対策ステップ、

を含むことを特徴とするセキュリティポリシー構築方法。

【請求項７】　請求項１記載のセキュリティポリシー構築方法において、

前記団体のセキュリティ状況を診断する診断ステップ、

を含み、前記診断ステップの診断結果を前記団体に提示することによって、前記団体がセキュリティポリシーの必要性を認識しうることを特徴とするセキュリティポリシー構築方法。

【請求項８】　請求項６記載のセキュリティポリシー構築方法において、

前記優先度と共に立てたセキュリティ対策の実行を、その優先度に合わせて計画し、団体の予算化を実現するプライオリティプランニングステップ、

を含むことを特徴とするセキュリティポリシー構築方法。

【請求項９】　請求項８記載のセキュリティポリシー構築方法において、
前記セキュリティ対策には、
セキュリティシステムの導入及びテストと、
セキュリティポリシーを遵守するための従業員の教育と、
システムログの分析と、
ネットワーク監視と、
セキュリティポリシーに基づく運用の監査と、
セキュリティポリシーの見直しと、
が含まれることを特徴とするセキュリティポリシー構築方法。

【請求項１０】　請求項８記載のセキュリティポリシー構築方法において、
前記計画に合わせて、前記セキュリティ対策を実行するセキュリティ強化策実行ステップ、
を含むことを特徴とするセキュリティポリシー構築方法。

【請求項１１】　セキュリティポリシーを構築する方法において、
団体に属するメンバーにするべき質問を生成する生成ステップと、
生成した前記質問を前記メンバーに聞く質問ステップと、
前記質問に対する前記メンバーの回答を取得する回答取得ステップと、
前記取得した回答に基づき、セキュリティポリシーを構築する構築ステップと、
を含むことを特徴とするセキュリティポリシー構築方法。

【請求項１２】　請求項１１記載のセキュリティポリシー構築方法において、
前記生成ステップは、被質問者の職務内容に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法。

【請求項１３】　請求項１１記載のセキュリティポリシー構築方法において、
前記回答取得ステップは、
前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管するステップと、

前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納するステップと、

前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を決定し、前記記憶手段中に回答群を格納するステップと、

の少なくとも１のステップを含むことを特徴とするセキュリティポリシー構築方法。

【請求項１４】　請求項１１記載のセキュリティポリシー構築方法において、

前記構築ステップは、

グローバルガイドラインに準拠して、前記団体の情報セキュリティに関する考え方、方針を記述するエグゼクティブレベルポリシーと、

前記エグゼクティブレベルポリシーを実現する情報セキュリティシステムの具体的な基準を記述するコーポレートレベルポリシーと、

前記エグゼクティブレベルポリシーの方針を、前記コーポレートレベルポリシーの基準に基づき実行するための手段を記述するプロダクトレベルポリシーと、

の３種類のセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法。

【請求項１５】　請求項１４記載のセキュリティポリシー構築方法において、

前記コーポレートレベルポリシーは、

前記団体全体の情報セキュリティシステムの基準を記述するトップレベルと、

前記団体の情報セキュリティシステムを構成する各ユニットの個々の基準を記述するサブレベルと、

の２種類のコーポレートレベルポリシーを含むことを特徴とするセキュリティポリシー構築方法。

【請求項１６】　請求項１４記載のセキュリティポリシー構築方法において、

前記プロダクトレベルポリシーは、

自然言語で記述された第１レベルと、

情報セキュリティシステムを構成する各構成装置の設定を記述する第２レベルと、

の２種類のプロダクトレベルポリシーを含むことを特徴とするセキュリティポリシー構築方法。

【請求項１７】　請求項１１記載のセキュリティポリシー構築方法において、

前記セキュリティポリシーのドラフトと、団体の実態との差異を調査する分析ステップ、

を含み、

前記分析ステップは、

前記取得した回答群中に矛盾する回答が含まれているか否かを検査する矛盾検査ステップと、

前記回答群によって仮想的に想定される情報システムと、前記セキュリティポリシーと、の比較をし差異を検査する第１差異検出ステップと、

前記回答群によって仮想的に想定される情報システムを実際の情報システムの調査でプルーフし、このプルーフした情報システムと、前記セキュリティポリシーのドラフトと、を比較をし差異を検査する第２差異検出ステップと、

の少なくとも１個のステップを含むことを特徴とするセキュリティポリシー構築方法。

【請求項１８】　請求項１７記載のセキュリティポリシー構築方法において、

前記調査した差異の対策をその優先度と共に立てる対策ステップ、

を含むことを特徴とするセキュリティポリシー構築方法。

【請求項１９】　セキュリティポリシーを構築するセキュリティポリシー構築装置において、

団体に属するメンバーにするべき質問を生成する質問生成手段と、

前記生成した質問に対する回答を保管する記憶手段と、

前記生成した質問に対する回答を取得し、前記記憶手段に保管する回答保管手

段と、

前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手段と、

を含むことを特徴とするセキュリティポリシー構築装置。

【請求項２０】　請求項１９記載のセキュリティポリシー構築装置において、

前記質問生成手段は、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とするセキュリティポリシー構築装置。

【請求項２１】　請求項１９記載のセキュリティポリシー構築装置において、

前記回答保管手段は、

前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、

または、

前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納し、

または、

前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を決定し、前記記憶手段中に回答群を格納する

ことを特徴とするセキュリティポリシー構築装置。

【請求項２２】　請求項１９記載のセキュリティポリシー構築装置において、

前記構築手段は、

前記団体の情報セキュリティに関する考え方、方針を記述するエグゼクティブレベルポリシーと、

前記エグゼクティブレベルポリシーを実現する情報セキュリティシステムの具体的な基準を記述するコーポレートレベルポリシーと、

前記エグゼクティブレベルポリシーの方針を、前記コーポレートレベルポリシ

ーの基準に基づき実行するための手段を記述するプロダクトレベルポリシーと、

の３種類のセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置。

【請求項２３】　請求項２２記載のセキュリティポリシー構築装置において、

前記コーポレートレベルポリシーは、

前記団体全体の情報セキュリティシステムの基準を記述するトップレベルと、

前記団体の情報セキュリティシステムを構成する各ユニットの個々の基準を記述するサブレベルと、

の２種類のコーポレートレベルポリシーを含むことを特徴とするセキュリティポリシー構築装置。

【請求項２４】　請求項２２記載のセキュリティポリシー構築装置において、

前記プロダクトレベルポリシーは、

自然言語で記述された第１レベルと、

情報セキュリティシステムを構成する各構成装置の設定を記述する第２レベルと、

の２種類のプロダクトレベルポリシーを含むことを特徴とするセキュリティポリシー構築装置。

【請求項２５】　団体のセキュリティ状況を評価する評価方法において、

前記団体に属するメンバーにするべき質問を生成する質問生成ステップと、

前記生成した質問を前記メンバーに聞く質問ステップと、

前記質問に対する前記メンバーの回答を取得する回答取得ステップと、

前記取得した回答に基づき、セキュリティ状況を評価するセキュリティ状況評価ステップと、

を含むことを特徴とする評価方法。

【請求項２６】　請求項２５記載の評価方法において、

前記質問生成ステップは、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とする評価方法。

【請求項２７】　請求項２５記載の評価方法において、

前記回答保管ステップは、

前記取得した回答が、以前に回答を得たことがある被質問者の回答であった場合に、前記以前の回答と、前記取得した回答とを統合し、単一の被質問者の回答として記憶手段中に保管することを特徴とする評価方法。

【請求項２８】　請求項２５記載の評価方法において、

前記セキュリティ状況の評価は、

前記団体のセキュリティの評価と、

前記団体が属する産業分野に含まれる他の団体のセキュリティの評価と、

前記団体が属する産業分野における団体が達成可能であると考えられるセキュリティの評価の最高値と、

を含むことを特徴とする評価方法。

【請求項２９】　請求項２５記載の評価方法において、

前記セキュリティ状況の評価は、

セキュリティに対する理解と姿勢、

前記団体のセキュリティ体制、

不測事態対応、

セキュリティに関する予算化、

セキュリティ改善措置、

の各項目に関する点数を含むことを特徴とする評価方法。

【請求項３０】　団体のセキュリティの状況を評価する評価装置において、

団体に属するメンバーにするべき質問を生成する生成手段と、

前記生成した質問に対する回答を保管する記憶手段と、

前記生成した質問に対する回答を取得し、前記記憶手段に保管する回答保管手段と、

前記保管した回答に基づき、団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成度作成手段と、

を含むことを特徴とする評価装置。

【請求項３１】　請求項３０記載の評価装置において、

前記生成手段は、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とする評価装置。

【請求項３２】　請求項３０記載の評価装置において、

前記回答保管手段は、

前記取得した回答が、以前に回答を得たことがある被質問者の回答であった場合に、前記以前の回答と、前記取得した回答とを統合し、単一の被質問者の回答として前記記憶手段中に保管することを特徴とする評価装置。

【請求項３３】　請求項３０記載の評価装置において、

前記セキュリティ完成度報告書は、

前記団体のセキュリティの完成度と、

前記団体が属する産業分野に含まれる他の団体のセキュリティの完成度と、

前記団体が属する産業分野における団体が達成可能であると考えられるセキュリティの完成度の最高値と、

を含むことを特徴とする評価装置。

【請求項３４】　請求項３０記載の評価装置において、

前記セキュリティ完成度報告書は、

セキュリティに対する理解と姿勢、

団体のセキュリティ体制、

不測事態対応、

セキュリティに関する予算化、

セキュリティ改善措置、

の各項目に関する点数を含むことを特徴とする評価装置。

【請求項３５】　セキュリティポリシーと、団体の情報システムとの差異を分析する分析装置において、

団体のメンバーに質問をすることによって得られた回答群に含まれる個々の回答の間に矛盾があるか否か検査する矛盾検査手段と、

前記検査した矛盾に関する情報を出力する矛盾出力手段と、

を含むことを特徴とする分析装置。

【請求項３６】　請求項３５記載の分析装置において、

前記矛盾に関する情報に基づき、前記回答群の整合をとり矛盾点を解決した回答群を生成する整合手段と、

前記整合手段が生成した回答群に基づき、団体の情報システムの構成を仮想的に構築する構築手段と、

前記仮想的に構築した情報システムの構成と、セキュリティポリシーとを比較し、両者の差異を出力する差異出力手段と、

を含むことを特徴とする分析装置。

【請求項３７】　請求項３６記載の分析装置において、

前記団体の情報システムを調査し、前記情報システムの構成を入力する実システム入力手段と、

前記情報システムの構成によって、前記仮想的に構成した情報システムをプルーフし、プルーフ後の前記仮想的に構成した情報システムの構成を、セキュリティポリシーとを比較し、両者の差異を出力する差異出力手段と、

を含むことを特徴とする分析装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、いわゆるセキュリティポリシーの構築に関する。特に、各団体に適合したセキュリティポリシーを迅速に構築可能な方法、及びセキュリティポリシーの構築を支援する装置に関する。

【０００２】

【従来の技術】

情報技術の発達と共に、情報セキュリティの重要性が増している。団体においては、団体内部の情報を保護するために種々の手段が講じられている。

【０００３】

たとえば、外部のネットワークと接続する部分にはいわゆるファイアーウォールを設け、他者が無断で内部のネットワークに侵入したり、内部の情報にアクセスしてしまうことを防止している。

【０００４】

また、コンピュータウィルス等を駆逐するために、ウィルス検出・駆除ソフトウェアに団体内部のコンピュータを監視させている。なお、本文においては、「団体」とは、企業の他、国や地方公共団体の機関、財団法人等各種法人、その他の団体・組織を意味する。

【０００５】

さて、上述したように、従来から種々の手段が情報セキュリティの確保のために用いられている。

【０００６】

しかしながら、各手段を別個独立に議論・検討していたのでは、団体全体としてのセキュリティ強度を確保することは困難である。

【０００７】

たとえば、いくらファイアーウォールを強化しても、団体の建物内に自由に第三者が入ってくることができ、そこにある端末を操作できるのであれば、団体全体としてのセキュリティ強度は著しく低下してしまう。

【０００８】

さらに、ウィルス検出ソフトウェアを用いていても、あらたなウィルスに対抗可能とするためにソフトウェアの更新を怠っていれば、新しいコンピュータウィルスには対抗できない。

【０００９】

したがって、団体全体としても情報セキュリティの強度を高くするためには、団体全体としての、情報セキュリティに対する設計及び実現手法を作りあげることが必要である。この設計及び実現手法（群）を一般にセキュリティポリシーと呼ぶ。

【００１０】

【発明が解決しようとする課題】

このセキュリティポリシーは、もちろん各団体毎に異なる項目、内容を有するものであるが、標準的なセキュリティポリシーを構築するための基本的な項目、内容が、国際的なガイドラインとして種々提案されている。

【００１１】

しかしながら、個々の団体毎にセキュリティポリシーを構築する必要がある。したがって、大量生産できるものではないため、セキュリティポリシーの構築には多大な労力と時間が必要であった。

【００１２】

さらに、セキュリティポリシーは、時間経過と共にその内容を変更する必要がある。たとえば、社内の組織が変更された場合には、それに応じて既存情報の利用価値やリスク評価の変更が生じ、それに見合ったセキュリティポリシーを変更しなければならない。

【００１３】

従来は、セキュリティポリシーの構築・定期的な修正等に関する一般的な手法は知られておらず、個々のシステムエンジニアが経験と勘に頼って、セキュリティポリシーの構築・修正を行っている。その結果、セキュリティポリシーの構築・修正に多大な労力が必要となってしまい、ともすれば、修正が団体と実状の変化に追いつけない事態も想定される。

【００１４】

したがって、セキュリティポリシーと団体の実状がかけ離れてしまい、強固な情報セキュリティを構築・維持することが困難な場合も見受けられた。

【００１５】

本発明は、係る課題に鑑みなされたものであり、その目的は、セキュリティポリシーを効率的に構築する方法及びセキュリティポリシーの構築を支援する装置を提供することである。

【００１６】

【課題を解決するための手段】

本発明は、上記課題を解決するために、所定の団体のセキュリティポリシーを構築する方法において、セキュリティポリシーのドラフトを構築するドラフト構築ステップと、前記セキュリティポリシーのドラフトと、団体の実態との差異を調査する分析ステップと、前記差異に基づき前記セキュリティポリシーのドラフトの調整、または、前記差異に基づき前記団体の実際の情報システムの運用ルールの調整、を行う調整ステップと、を含むことを特徴とするセキュリティポリシ

ー構築方法である。

【００１７】

このような構成によって、セキュリティポリシーの構築を段階的に行うことができ、効率的なセキュリティポリシーの構築を行うことができる。

【００１８】

また、本発明は、前記ドラフト構築ステップは、団体に属するメンバーにするべき質問を生成する生成ステップと、生成した前記質問を前記メンバーに聞く質問ステップと、前記質問に対する前記メンバーの回答を取得する回答取得ステップと、前記取得した回答に基づき、セキュリティポリシーのドラフトを構築する構築ステップと、を含むことを特徴とするセキュリティポリシー構築方法である。

【００１９】

このような構成によって、質問に基づきセキュリティポリシーのドラフトを構築できる。

【００２０】

また、本発明は、前記生成ステップは、被質問者の職務内容に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法である。

【００２１】

職務内容に基づき、質問が生成されるため、効率的な質問を行うことが可能である。

【００２２】

また、本発明は、前記回答取得ステップは、前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管するステップと、前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納するステップと、前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を決定し、前記記憶手段中に回答群を格納するステップと、の少なくとも１のステップを含むことを特徴とするセキュリティポリシー構築方法である。

【００２３】

このような構成によって、複数人で分散して質問をした場合に、得られた回答を統合することが可能である。

【００２４】

また、本発明は、前記分析ステップは、前記取得した回答群中に矛盾する回答が含まれているか否かを検査する矛盾検査ステップと、前記回答群によって仮想的に想定される情報システムと、前記セキュリティポリシーと、の比較をし差異を検査する第１差異検出ステップと、前記回答群によって仮想的に想定される情報システムを実際の情報システムの調査でプルーフし、このプルーフした情報システムと、前記セキュリティポリシーのドラフトと、を比較をし差異を検査する第２差異検出ステップと、の少なくとも１のステップを含むことを特徴とするセキュリティポリシー構築方法である。

【００２５】

このような構成によって、回答間の矛盾を知ることができ、さらに、実システムとセキュリティポリシーの差異を検出することが可能である。

【００２６】

また、本発明は、前記調査した差異の対策をその優先度と共に立てる対策ステップ、を含むことを特徴とするセキュリティポリシー構築方法である。

【００２７】

このような構成によって、優先度を含めた対策を講じることが可能である。

【００２８】

また、本発明は、前記団体のセキュリティ状況を診断する診断ステップ、を含み、前記診断ステップの診断結果を前記団体に提示することによって、前記団体がセキュリティポリシーの必要性を認識しうることを特徴とするセキュリティポリシー構築方法である。

【００２９】

このような構成によって、団体のセキュリティ状況を知ることができる。

【００３０】

また、本発明は、前記優先度と共に立てたセキュリティ対策の実行を、その優

先度に合わせて計画し、団体の予算化を実現するプライオリティプランニングステップ、を含むことを特徴とするセキュリティポリシー構築方法である。

【００３１】

このような構成によって、セキュリティ対策を計画的に実行することができ、予算を立てることが容易となる。

【００３２】

また、本発明は、前記セキュリティ対策には、セキュリティシステムの導入及びテストと、セキュリティポリシーを遵守するための従業員の教育と、システムログの分析と、ネットワーク監視と、セキュリティポリシーに基づく運用の監査と、セキュリティポリシーの見直しと、が含まれることを特徴とするセキュリティポリシー構築方法である。

【００３３】

情報セキュリティ機器の導入だけでなく、従業員の教育等も行ったため、高い情報セキュリティを達成することができる。

【００３４】

また、本発明は、前記計画に合わせて、前記セキュリティ対策を実行するセキュリティ強化策実行ステップ、を含むことを特徴とするセキュリティポリシー構築方法である。

【００３５】

このような構成によって、セキュリティ対策を円滑に実行に移すことが可能である。

【００３６】

また、本発明は、セキュリティポリシーを構築する方法において、団体に属するメンバーにするべき質問を生成する生成ステップと、生成した前記質問を前記メンバーに聞く質問ステップと、前記質問に対する前記メンバーの回答を取得する回答取得ステップと、前記取得した回答に基づき、セキュリティポリシーを構築する構築ステップと、を含むことを特徴とするセキュリティポリシー構築方法である。

【００３７】

このような構成によって、質問に基づきセキュリティポリシーのドラフトを構築できる。

【００３８】

また、本発明は、前記生成ステップは、被質問者の職務内容に基づき、前記質問を生成することを特徴とするセキュリティポリシー構築方法である。

【００３９】

職務内容に基づき、質問が生成されるため、効率的な質問を行うことが可能である。

【００４０】

また、本発明は、前記回答取得ステップは、前記取得した回答群中で、被質問者が同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管するステップと、前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納するステップと、前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を決定し、前記記憶手段中に回答群を格納するステップと、の少なくとも１のステップを含むことを特徴とするセキュリティポリシー構築方法である。

【００４１】

このような構成によって、複数のエンジニアで分散してインタビューをした場合に、その回答のを整合性をとり、インタビュー結果を統合可能である。

【００４２】

また、本発明は、前記構築ステップは、前記団体の情報セキュリティに関する考え方、方針を記述するエグゼクティブレベルポリシーと、前記エグゼクティブレベルポリシーを実現する情報セキュリティシステムの具体的な基準を記述するコーポレートレベルポリシーと、前記エグゼクティブレベルポリシーの方針を、前記コーポレートレベルポリシーの基準に基づき実行するための手段を記述するプロダクトレベルポリシーと、の３種類のセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築方法である。

【００４３】

３種類のセキュリティポリシーが構築されるため、階層的なセキュリティポリシーを得ることができる。ここで、前記コーポレートレベルポリシーの基準に基づき実行するための手段とは、ハードウェア・ソフトウェアだけでなく、それらを利用する際の運用ルール等も含む。

【００４４】

また、本発明は、前記コーポレートレベルポリシーは、前記団体全体の情報セキュリティシステムの基準を記述するトップレベルと、前記団体の情報セキュリティシステムを構成する各ユニットの個々の基準を記述するサブレベルと、の２種類のコーポレートレベルポリシーを含むことを特徴とするセキュリティポリシー構築方法である。

【００４５】

このような構成によって団体全体のセキュリティポリシーと、個別の機器のセキュリティポリシーとを明確にすることができる。ここで、機器とは、ネットワーク、ホスト、アプリケーション、を含む概念である。

【００４６】

また、本発明は、前記プロダクトレベルポリシーは、自然言語で記述された第１レベルと、情報セキュリティシステムを構成する各構成装置の設定を記述する第２レベルと、の２種類のプロダクトレベルポリシーを含むことを特徴とするセキュリティポリシー構築方法である。

【００４７】

このように、第１レベルのプロダクトレベルポリシーによって、人間がセキュリティポリシーを理解することができ、さらに第２レベルのプロダクトレベルポリシーによって各装置の設定が容易になる。ここで、構成装置は、情報セキュリティシステムを構成するハードウェア・ソフトウェアを含むものである。

【００４８】

また、本発明は、前記分析ステップは、前記取得した回答群中に矛盾する回答が含まれているか否かを検査する矛盾検査ステップと、前記回答群によって得られた団体の情報システムと、団体の実際の情報システムとの間に差異があるか否かを調査する差異検出ステップと、を含むことを特徴とするセキュリティポリシ

ー構築方法である。

【００４９】

このような構成によって、矛盾点や、差異を効率的に検出することができる。

【００５０】

また、本発明は、前記調査した差異の対策をその優先度と共に立てる対策ステップ、を含むことを特徴とするセキュリティポリシー構築方法である。

【００５１】

対策がその優先度と共に立てられるため、情報セキュリティの構築計画を立案するのが容易になる。

【００５２】

また、本発明は、団体に属するメンバーにするべき質問を生成する質問生成手段と、前記生成した質問に対する回答を保管する記憶手段と、前記生成した質問に対する回答を取得し、前記記憶手段に保管する回答保管手段と、前記記憶手段に保管される前記回答に基づき、セキュリティポリシーを構築する構築手段と、を含むことを特徴とするセキュリティポリシー構築装置である。

【００５３】

このような構成によれば、メンバーに対する質問が生成されるため、質問作業が容易になる。なお、メンバーとは、その団体の情報システムに関連する個人を意味する。たとえば、従業員だけでなく、パートタイムワーカーや、関連会社の社員等も含まれる。

【００５４】

また、本発明は、前記質問生成手段は、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とするセキュリティポリシー構築装置である。

【００５５】

職務内容に基づき、質問が生成されるため、効率的な質問を行うことが可能である。

【００５６】

また、本発明は、前記回答保管手段は、前記取得した回答群中で、被質問者が

同一である回答を統合し、単一の被質問者の回答として前記記憶手段中に保管し、または、前記取得した回答群中に矛盾する回答が含まれている場合には、再質問を実行し、矛盾点を解決し、前記記憶手段中に前記回答群を格納し、または、前記取得した回答群中に矛盾する回答が含まれている場合には、前記回答に被質問者の職務内容に基づく重み付けをすることによって、回答を決定し、前記記憶手段中に回答群を格納することを特徴とするセキュリティポリシー構築装置である。

【００５７】

このような構成によって、複数のエンジニアで分散してインタビューをした場合に、整合性をとり、統合可能である。

【００５８】

また、本発明は、前記構築手段は、前記団体の情報セキュリティに関する考え方、方針を記述するエグゼクティブレベルポリシーと、前記エグゼクティブレベルポリシーを実現する情報セキュリティシステムの具体的な基準を記述するコーポレートレベルポリシーと、前記エグゼクティブレベルポリシーの方針を、前記コーポレートレベルポリシーの基準に基づき実行するための手段を記述するプロダクトレベルポリシーと、の３種類のセキュリティポリシーを構築することを特徴とするセキュリティポリシー構築装置である。

【００５９】

３種類のセキュリティポリシーが構築されるため、階層的なセキュリティポリシーを得ることができる。ここで、前記コーポレートレベルポリシーの基準に基づき実行するための手段とは、ハードウェア・ソフトウェアだけでなく、それらを利用する際の運用ルール等も含む。

【００６０】

また、本発明は、前記コーポレートレベルポリシーは、前記団体全体の情報セキュリティシステムの基準を記述するトップレベルと、前記団体の情報セキュリティシステムを構成する各ユニットの個々の基準を記述するサブレベルと、の２種類のコーポレートレベルポリシーを含むことを特徴とするセキュリティポリシー構築装置である。

【００６１】

このような構成によって団体全体のセキュリティポリシーと、個別の機器のセキュリティポリシーとを明確にすることができる。ここで、機器とは、ネットワーク、ホスト、アプリケーション、を含む概念である。

【００６２】

また、本発明は、前記プロダクトレベルポリシーは、自然言語で記述された第１レベルと、情報セキュリティシステムを構成する各装置の設定を記述する第２レベルと、の２種類のプロダクトレベルポリシーを含むことを特徴とするセキュリティポリシー構築装置である。

【００６３】

このように、第１レベルのプロダクトレベルポリシーによって、人間がセキュリティポリシーを理解することができ、さらに第２レベルのプロダクトレベルポリシーによって各装置の設定が容易になる。ここで、構成装置は、情報セキュリティシステムを構成するハードウェア・ソフトウェアを含む。

【００６４】

また、本発明は、団体のセキュリティ状況を評価する評価方法において、前記団体に属するメンバーにするべき質問を生成する質問生成ステップと、前記生成した質問を前記メンバーに聞く質問ステップと、前記質問に対する前記メンバーの回答を取得する回答取得ステップと、前記取得した回答に基づき、セキュリティ状況を評価するセキュリティ状況評価ステップと、を含むことを特徴とする評価方法である。

【００６５】

このような構成によって、質問に対する回答に基づき、団体のセキュリティの状況を知ることが可能である。

【００６６】

また、本発明は、前記質問生成ステップは、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とする評価方法である。

【００６７】

職務内容に基づき、質問が生成されるため、効率的な質問を行うことが可能で

ある。

【００６８】

また、本発明は、前記回答保管ステップは、前記取得した回答が、以前に回答を得たことがある被質問者の回答であった場合に、前記以前の回答と、前記取得した回答とを統合し、単一の被質問者の回答として記憶手段中に保管することを特徴とする評価方法である。

【００６９】

このような構成によって、複数のエンジニアで分散してインタビューをした場合に、その回答のを整合性をとり、インタビュー結果を統合可能である。

【００７０】

また、本発明は、前記セキュリティ状況の評価は、前記団体のセキュリティの評価と、前記団体が属する産業分野に含まれる他の団体のセキュリティの評価と、前記団体が属する産業分野における団体が達成可能であると考えられるセキュリティの評価の最高値と、を含むことを特徴とする評価方法である。

【００７１】

このような構成によって、その団体を他社と比較して評価することが可能である。また、理論上の最高値が示されるので、達成すべき目標を定めやすくなる。

【００７２】

また、本発明は、前記セキュリティ状況の評価は、セキュリティに対する理解と姿勢、前記団体のセキュリティ体制、不測事態対応、セキュリティに関する予算化、セキュリティ改善措置、の各項目に関する点数を含むことを特徴とする評価方法である。

【００７３】

このような構成によって、団体の情報セキュリティの評価を項目別に知ることが可能である。

【００７４】

また、本発明は、団体のセキュリティの状況を評価する評価装置において、団体に属するメンバーにするべき質問を生成する生成手段と、前記生成した質問に対する回答を保管する記憶手段と、前記生成した質問に対する回答を取得し、前

記記憶手段に保管する回答保管手段と、前記保管した回答に基づき、団体のセキュリティの完成度を表すセキュリティ完成度報告書を作成するセキュリティ完成度作成手段と、を含むことを特徴とする評価装置である。

【００７５】

このような構成によって、生成された質問をメンバーに行い、質問に対する回答に基づき、団体のセキュリティの状況を知ることが可能である。

【００７６】

また、本発明は、請求項３０記載の評価装置において、前記生成手段は、被質問者の職務内容に基づき、前記被質問者にするべき質問を生成することを特徴とする評価装置である。

【００７７】

職務内容に基づき、質問が生成されるため、効率的な質問を行うことが可能である。

【００７８】

また、本発明は、前記回答保管手段は、前記取得した回答が、以前に回答を得たことがある被質問者の回答であった場合に、前記以前の回答と、前記取得した回答とを統合し、単一の被質問者の回答として前記記憶手段中に保管することを特徴とする評価装置である。

【００７９】

このような構成によって、複数人で質問をした場合に、得られた回答を統合することが可能である。

【００８０】

また、本発明は、前記セキュリティ完成度報告書は、前記団体のセキュリティの完成度と、前記団体が属する産業分野に含まれる他の団体のセキュリティの完成度と、前記団体が属する産業分野における団体が達成可能であると考えられるセキュリティの完成度の最高値と、を含むことを特徴とする評価装置である。

【００８１】

このような構成によって、その団体を他社と比較して評価することが可能である。また、理論上の最高値が示されるので、目標を設定することが容易となる。

【００８２】

また、本発明は、前記セキュリティ完成度報告書は、セキュリティに対する理解と姿勢、団体のセキュリティ体制、不測事態対応、セキュリティに関する予算化、セキュリティ改善措置、の各項目に関する点数を含むことを特徴とする評価装置である。

【００８３】

このような構成によって、団体の情報セキュリティの評価を項目別に知ることが可能である。

【００８４】

また、本発明は、セキュリティポリシーと、団体の情報システムとの差異を分析する分析装置において、団体のメンバーに質問をすることによって得られた回答群に含まれる個々の回答の間に矛盾があるか否か検査する矛盾検査手段と、前記検査した矛盾に関する情報を出力する矛盾出力手段と、を含むことを特徴とする分析装置である。

【００８５】

このような構成によって、回答群中に含まれる矛盾を知ることが可能である。

【００８６】

また、本発明は、前記矛盾に関する情報に基づき、前記回答群の整合をとり矛盾点を解決した回答群を生成する整合手段と、前記整合手段が生成した回答群に基づき、団体の情報システムの構成を仮想的に構築する構築手段と、前記仮想的に構築した情報システムの構成と、セキュリティポリシーとを比較し、両者の差異を出力する差異出力手段と、を含むことを特徴とする分析装置である。

【００８７】

このような構成によって、セキュリティポリシーと団体の実態との差異を知ることができる。

【００８８】

また、本発明は、前記団体の情報システムを調査し、前記情報システムの構成を入力する実システム入力手段と、前記情報システムの構成によって、前記仮想的に構成した情報システムをプルーフし、プルーフ後の前記仮想的に構成した情

報システムの構成を、セキュリティポリシーとを比較し、両者の差異を出力する差異出力手段と、を含むことを特徴とする分析装置である。

【００８９】

このような構成によって、実際の調査によってプルーフした情報システムとセキュリティポリシーの比較を行っているので、両者の差異をより正確に分析することができる。

【００９０】

【発明の実施の形態】

以下、本発明の好適な実施の形態を図面に基づいて説明する。

【００９１】

ある団体に対して行うセキュリティポリシーの構築からそのメンテナンスに至る一連の作業を含むビジネスモデルについて説明する。このビジネスモデルは一般にはシステムエンジニアが所定のエキスパートシステムを用いて実行することが好ましい。

【００９２】

本実施の形態におけるビジネスモデルの原理をまず説明する。図１には、このビジネスモデルの原理を表すフローチャートが示されている。この図に示すように、本ビジネスモデルは、基本的には６個のステップから構成される。

【００９３】

ステップ１　セキュリティ完成度評価

ステップ２　セキュリティポリシードラフト構築

ステップ３　システム及びその運用の実査・分析

ステップ４　ポリシー調整・ルール調整

ステップ５　プライオリティプランニング

ステップ６　セキュリティ強化策実行

このような６段階のステップからなるセキュリティ構築手法によれば、最初はインタビューベースのセキュリティポリシーのドラフトを構築し、必要に応じ、団体の実態との再調整を行い、段階的にセキュリティポリシーを完成していくので、各団体のスケジュールや予算に合わせてセキュリティポリシーを構築するこ

とが可能である。

【００９４】

ステップ１は、団体の情報セキュリティの現状を評価するステップである。この評価によって、団体は自社の情報セキュリティの現状を知ることができる。

【００９５】

ステップ２は、団体のメンバーに対して質問をすることによって簡易にセキュリティポリシーのドラフトを作成するステップである。単にインタビューによってセキュリティポリシーのドラフトを作成しているので、安価にセキュリティポリシーを作成することができる。

【００９６】

ステップ３は、セキュリティポリシーのドラフトと、団体の実態との相違を検討するステップである。ドラフトは質問に対する回答にのみ基づき作成されているので、実態との相違が生じる場合があるからである。

【００９７】

ステップ４は、差異に基づいて、セキュリティポリシーを調整又は導入済みのセキュリティ商品のルールを調整するステップである。

【００９８】

ステップ５は、今後の情報セキュリティ計画を、各手段や対策を採用する優先度も含めて構築するステップである。

【００９９】

ステップ６は、この計画に基づいて、必要なセキュリティ保護対策を実施するステップである。

【０１００】

以上のように段階的にセキュリティポリシーの構築を行っているため、各団体の予算や考え方等の実状に合わせたセキュリティポリシーの構築が可能である。

【０１０１】

たとえば、小規模な団体ではセキュリティポリシーのドラフトで十分な場合もあろう。また、プライオリティプランニングによれば、将来の計画がわかるため、団体の予算を立てやすくなるというメリットがある。

【０１０２】

特に、本ビジネスモデルについて中心的なステップは、ステップ２～ステップ４である。ステップ２においてドラフトを作成し、ステップ３において実態との差異を分析し、ステップ４においてセキュリティポリシー又は導入済みのセキュリティ商品の調整を行う。少なくともこれらステップ２～ステップ４を含むビジネスモデルであれば、セキュリティポリシーの構築をシステマティックに行うことができ、従来の経験と勘に頼る手法に比べて、生産性及び品質を高めることが可能である。

【０１０３】

また、このような段階的なセキュリティポリシーの構築を実現するために、本実施の形態では、種々のエキスパートシステムを使用している。

【０１０４】

以下、エキスパートシステムの利用方法も含めて、ステップ１～ステップ６の各ステップを順に説明する。

【０１０５】

Ａ．ステップ１：セキュリティ完成度評価

このステップでは、団体の現在の情報セキュリティに関する客観的な評価を行う。このような評価を行うことによって、セキュリティに関する団体のランク付けを行うことが可能である。なお、具体的には、上記評価は、セキュリティ完成度評価書を作成することによって実行される。

【０１０６】

本実施の形態では、米国カーネギーメロン大学のSoftware Capability Maturity Modelに基づき、セキュリティ完成度評価を行う。このModelでは、５個の項目に対して定量的評価を行う。すなわち、点数を与えるのである。

【０１０７】

５個の項目は、以下の通りである。

【０１０８】

ａ．情報セキュリティに対する管理者の理解と姿勢

ｂ．団体のセキュリティ状況

ｃ．不測事態対応

ｄ．セキュリティに関する予算化

ｅ．セキュリティ改善措置

ここで、不測事態とは、情報セキュリティを脅かす事象をいう。たとえば、盗聴行為、機器の故障等である。これらの不測事態に対応できる体制にあるか否かを表すのが上記ｃ．不測事態対応である。また、ｄ．予算化とは、情報セキュリティのために予算が十分にとられているか否かを表す。また、ｅ．セキュリティ改善措置とは、セキュリティの改善の予定や計画がどの程度立てられているか、を表す。

【０１０９】

本実施の形態では、このような５個の項目に関する点数付けを含む完成度評価書を作成することによって、団体のセキュリティに関する現在の状況を知ることが可能である。

【０１１０】

具体的なセキュリティ完成度評価書の作成手法について説明する。

【０１１１】

本実施の形態では、団体に属するメンバーに質問をし、その回答に基づいて、完成度評価書を作成する。具体的には、図２に示すような評価装置１０を用いて、質問の生成、回答の収集、セキュリティ完成度評価書の作成等を実行している。また、評価書の作成作業の動作を表すフローチャートが図３に示されている。この図３に示されているフローチャートは、図１におけるステップＳ１－１をより詳細に表したフローチャートである。

【０１１２】

まず、図２に示すように、評価装置１０は、被質問者の職務内容に基づいて、行うべき質問を生成する質問生成手段１２を備えている。たとえば、社長にウイルス検査プログラムについて聞いてもあまり意味がなく、また、新入社員に情報セキュリティの予算について聞いても有意義な回答を得るのは困難である。

【０１１３】

そこで、質問生成手段１２は、その被質問者の職務内容に応じて、するべき質

問を記憶手段１４から抽出するのである。記憶手段１４には、あらかじめ多種多様な質問が格納されており、被質問者に必要な質問が質問生成手段１２によって抽出されるのである。

【０１１４】

本実施の形態において特徴的なことは、このようにそのメンバーの職務内容によって生成する質問が変更されることである。その結果、被質問者に対して行うべき適切な質問を生成することが可能である。

【０１１５】

メンバーの職務内容によって決定されるのは、質問群のいわばコースである。各コースにおいて出される質問は、メンバーの回答内容によって変更される。たとえば、ＶＰＮを使用しているかという質問に対して、使用していないと回答すれば、ＶＰＮの詳細に関する質問はスキップされる。しかし、ＶＰＮを使用していると回答した場合には、その回答をしたメンバーには、ＶＰＮの詳細に関する質問がなされる。

【０１１６】

このような制御は、いわゆる知識ベースのエキスパートシステムを利用して実行される。

【０１１７】

また、評価装置１０は、回答保管手段１６を備えている。上記のようにして生成した質問を団体に属するメンバーに提示して得られた回答は、この回答保管手段１６に供給される。回答保管手段１６は、回答を記憶手段１４に保管する。

【０１１８】

本実施の形態において特徴的なことは、回答保管手段１６が回答の統合機能を有していることである。この統合機能とは、質問を複数人のシステムエンジニアが行った場合に、その回答を１個のデータベースにまとめて記憶手段１４に保管する機能である。質問をするべきメンバーが多数いる場合には、複数人のシステムエンジニアが分担してインタビュー質問を行ったほうが迅速に質問に対する回答を得ることができる。このように質問を分担して実行した場合に、その結果は複数のコンピュータ上にそれぞれ蓄積される。したがって、これらの結果を統合

する必要があるのである。

【０１１９】

もちろん、ある１人のメンバーに対する質問や回答が一度にできず、複数回に分けて行われた場合に、それらの結果を統合するためにも利用可能である。

【０１２０】

また、評価装置１０は、セキュリティ完成度報告書の作成を行うセキュリティ完成度作成手段１８を備えている。このセキュリティ完成度作成手段１８は、記憶手段１４に保管されている回答群に基づきその団体の情報セキュリティに関する評価書であるセキュリティ完成度報告書を作成する。

【０１２１】

この評価装置１０はいわゆるエキスパートシステムである。

【０１２２】

特に、上述したように、本実施の形態では、職務内容に応じて質問を変更し、さらに、収集した回答を統合する機能等を備える評価装置１０を採用している。したがって、セキュリティ完成度評価書を効率よくしかも精密に作成することが可能である。

【０１２３】

次に、図３のフローチャートに基づき、セキュリティ完成度評価書の作成動作について説明する。

【０１２４】

まず、ステップＳ３－１においては、被質問者であるメンバーの職務内容を質問生成手段１２に供給し、そのメンバーに対して行う質問を生成する。

【０１２５】

そして、ステップＳ３－２において、システムエンジニアは得られた質問をメンバーに対して行う。

【０１２６】

ステップＳ３－３においては、質問に対する回答をメンバーから得て、評価装置１０の回答保管手段１６に供給する。回答保管手段１６は上述のように統合機能を有しており、同一のメンバーからの回答を統合して記憶手段１４に格納する

。このような統合機能によって、複数のシステムエンジニアがそれぞれ得てきた回答群を、まとめて一つの記憶手段１４に格納することができる。

【０１２７】

統合機能

統合機能は、以下のような機能を含んでいる。

【０１２８】

（１）複数のエンジニアが、分散してメンバーにインタビューを行い、インタビュー結果である回答を収集し、一つのデータベースにまとめる。たとえば、ある１人のメンバーに複数のエンジニアがインタビューをした場合には、それらの回答は１のデータベースに統合される。また、たとえば、同種類（たとえばネットワーク）に関する一連の質問を、複数のメンバーにした場合、それらの回答を統合して１のデータベースに組み込む。

【０１２９】

（２）インタビューにおいては同一の質問が異なるメンバーになされる場合がある。その結果、回答に矛盾が生じる場合も考えられる。この矛盾を解決するためには、２つの手法がある。第１の手法は、再インタビューである。矛盾点に関し、回答者に言い間違い等があったばあいには、再インタビュー又は実査（またはそれら双方）を実行することにより矛盾点を解決できると考えられる。第２の手法は、タイプ（職務内容）によるウェイト付けで、回答を定める方法である。

【０１３０】

本実施の形態においては、利用者はこの第１の手法と第２の手法を自由に選択することができる。再インタビューをする時間がある場合には第１の手法が好ましいが、インタビューの対象者が多すぎる場合には、第２の手法が好ましい。

【０１３１】

さて、ステップＳ３－４においては、セキュリティ完成度作成手段１８が記憶手段１４に格納された回答群に基づいて、上記の５項目に関するスコア（点数）を含むセキュリティ完成度評価書を作成する。

【０１３２】

以上のようにして、評価装置１０を用いて、セキュリティ完成度評価書が作成

される。

【０１３３】

業界標準との比較

セキュリティ完成度評価書には、上述したように、５個の項目に関するスコア（点数）が示される。

【０１３４】

特に、本実施の形態において特徴的なことは、その団体の属する業界における全団体の平均的なスコア及び最高のスコアが併せて表示されることである。ここで、最高のスコアとは、その業界に含まれる団体であれば達成できるであろう最高のスコア（理論値）である。

【０１３５】

これによって、その団体の情報セキュリティに対する取り組みが、その業界の中でどの程度の位置にいるかを容易に知ることが可能である。なお、このような業界の平均値や最高値は、記憶手段１４にあらかじめ格納してある。さらに、平均値は、セキュリティ完成度評価を実行して、ある団体のスコアを算出するたびに更新される。

【０１３６】

地理的な側面の検討

なお、本実施の形態においては、質問の内容に地域的な考慮をした質問も含まれている。たとえば、商品の主な市場は国内か、海外か、等の質問が含まれている。また、主な取引先はどこか、等の質問も含まれている。このような質問が含まれていることによって、情報セキュリティの完成度を評価する際に地域的な考慮を加えることが可能となる。なお、これは地域によってセキュリティ格差があることを考慮したものである。

【０１３７】

セキュリティ実装の経緯報告

本実施の形態では、セキュリティ完成度評価書は、セキュリティポリシーの構築を行う前に団体の情報セキュリティの実態を調査する趣旨で作成している。しかし、情報セキュリティの対策を順次実行していく途中段階で適宜このセキュリ

ティ完成度報告書を作成すれば、情報セキュリティ対策の進捗の程度を知ることが可能である。したがって、このセキュリティ完成度報告書の作成ステップは、セキュリティ実装の経緯報告としての性格も有する。

【０１３８】

なお、本実施の形態の評価装置１０では、質問や回答などがすべて記憶手段１４に格納されているが、それぞれ専用の別個の記憶手段に格納してもかまわない。

【０１３９】

Ｂ．ステップ２：セキュリティポリシードラフト構築

このステップでは、その団体のセキュリティポリシーの簡単なドラフトを構築する。このドラフトは、団体に属するメンバーに質問をし、その回答に基づき構築するセキュリティポリシーである。したがって、団体の実際の情報システムの調査を行っていないため、迅速にセキュリティポリシーの構築を行うことができる。

【０１４０】

標準的なセキュリティポリシーを構築するための基本的な項目、内容が国際的なガイドラインとして種々知られている。これらをグローバルガイドラインと呼ぶ。本実施の形態では、これらグローバルガイドライン中の原則を、適宜取り出し、組み合わせることによって、セキュリティポリシーのドラフトを構築する。

【０１４１】

本実施の形態では、セキュリティポリシードラフト構築装置２０を利用してセキュリティポリシーのドラフトを構築している。このセキュリティポリシードラフト構築装置２０の構成ブロック図が図４に示されている。

【０１４２】

セキュリティポリシードラフト構築装置２０は、図４に示すように、被質問者の職務内容に基づいて、行うべき質問を生成する質問生成手段２２を備えている。このように職務内容に基づいて、質問を変更するのは、上記評価装置１０の質問生成手段１２と同様に、有意義な回答を得るためである。

【０１４３】

また、図２の記憶手段１４と同様に、セキュリティポリシードラフト構築装置２０内の記憶手段２４にも、多種多様な質問があらかじめ格納されている。そして、質問生成手段２２が、メンバーの職務内容に応じて適切な質問を記憶手段２４から抽出するのである。

【０１４４】

また、セキュリティポリシードラフト構築装置２０は、回答保管手段２６を備えている。この回答保管手段２６も、上記回答保管手段１６と同様に回答を記憶手段２４に保管する。また、回答保管手段２６は、上記回答保管手段１６と同様に回答の統合機能を有している。

【０１４５】

また、セキュリティポリシードラフト構築装置２０は、セキュリティポリシーのドラフトを構築するドラフト構築手段２８を備えている。このドラフト構築手段２８は、記憶手段２４に保管されている回答群に基づきそのセキュリティポリシーのドラフトを作成する。

【０１４６】

このセキュリティポリシードラフト構築装置２０も、評価装置１０と同様にいわゆるエキスパートシステムであり、実際には上記各手段は、コンピュータ上で動作するソフトウェアによって実現することが好ましい。

【０１４７】

次に、図５のフローチャートに基づき、セキュリティポリシーのドラフトを構築する動作を説明する。図５には、セキュリティポリシードラフト構築装置２０を用いてセキュリティポリシーのドラフトを構築する動作を表すフローチャートが示されている。

【０１４８】

まず、ステップＳ５－１においては、被質問者であるメンバーの職務内容を質問生成手段２２に供給し、そのメンバーに対して行う質問を生成する。

【０１４９】

本実施の形態においては、このようにそのメンバーの職務内容によって生成する質問が決定される。その結果、被質問者に対して行うべき適切な質問を生成す

ることが可能である。

【０１５０】

メンバーの職務内容によって決定されるのは、質問群のいわばコースである。各コースにおいて出される実際の質問は、メンバーの回答内容によって変更される。たとえば、ＶＰＮを使用しているかという質問に対して、使用していないと回答すれば、ＶＰＮの詳細に関する質問はスキップされる。しかし、ＶＰＮを使用していると回答した場合には、その回答をしたメンバーには、ＶＰＮの詳細に関する質問がなされる。

【０１５１】

このような制御は、いわゆる知識ベースのエキスパートシステムを利用して実行される。

【０１５２】

ステップＳ５－２において、生成した質問をメンバーに対して行う。

【０１５３】

ステップＳ５－３においては、質問に対する回答をメンバーから得て、セキュリティポリシードラフト構築装置２０の回答保管手段２６に入力する。入力作業はシステムエンジニアが行うのが好ましい。もちろん、質問を受ける各メンバーがポリシードラフト構築装置２０の画面に向かって、表示される質問に答えるような形態を採用してもかまわない。回答保管手段２６は上述のように統合機能を有しており、複数のシステムエンジニアが取得してきた回答を統合して、記憶手段２４に格納する。

【０１５４】

ステップＳ５－４においては、ドラフト構築手段２８が記憶手段２４に格納された回答群に基づいて、グローバルガイドライン中の原則を種々組み合わせてセキュリティポリシーを構築する。

【０１５５】

以上のようにして、セキュリティポリシードラフト構築装置２０を用いて、セキュリティポリシーのドラフトが作成される。

【０１５６】

なお、本実施の形態では、エグゼクティブレベルポリシー、コーポレートレベルポリシー、プロダクトレベルポリシーの３種類のセキュリティポリシー（のドラフト）が構築される。これら３種類に関する説明は、Ｂ－５章において後述する。

【０１５７】

Ｂ－１：質問（インタビュー）の内容

以下、質問（以下、インタビューとも呼ぶ）の内容について説明する。

【０１５８】

インタビュー大項目は、以下の通りである。

【０１５９】

１．企業

２．ネットワーク

３．サーバとホスト

４．アプリケーションとデータベース

５．重要性の高いセキュリティ項目

６．補正項目

以下、各項目を説明する。

【０１６０】

（１）企業

項目「企業」では、典型的な団体の一つである「企業」の概要、体制に関するインタビューが実行される。このインタビュー質問の回答から、情報セキュリティの管理体制、ポリシーの原則、脆弱性分析等を導くことが可能である。

【０１６１】

項目「企業」には、さらに小項目として、以下の項目が含まれている。

【０１６２】

１．１　管理体制

１．２　従業員

１．３　会社概要

１．４　ベンダー

１．５　顧客

１．６　コンサルタント

１．７　外部委託

１．８　アプリケーション

１．９　ネットワーク

１．１０　セキュリティプロファイル

１．１１　業種

１．１２　団体ポリシー

ただし、職務内容によって質問項目が異なる。たとえば、最高経営責任者にはホストについての質問項目はない。このように、本実施の形態において特徴的なことは、職務によって質問内容が異なることである。これによって、その職務内容に応じた質問をすることができ、効率的なインタビューが可能である。

【０１６３】

（２）ネットワーク

項目「ネットワーク」では、ネットワークの概要、運用、設定に関するインタビュー質問が実行される。このインタビュー質問の回答から、ネットワークの脆弱性、ネットワークに関するコーポレートレベルポリシー等が導かれる。

【０１６４】

ネットワークに含まれる質問群は、多くはコーポレートレベルポリシーに影響を与える質問であるが、プロダクトレベルポリシーに影響を与える質問もある。

【０１６５】

項目「ネットワーク」には、さらに小項目として、以下の項目が含まれている。

【０１６６】

２．１　運用環境

２．２　ネットワークのプロパティ

２．３　認証と識別

２．４　監査とログ

２．５　アクセス制御

２．６　変更手続き

２．７　災害復旧とバックアップ

２．８　オペレーションの信頼性

２．９　物理的セキュリティ

２．１０　モデム

２．１１　ワークステーションセキュリティ

（３）サーバとホスト

項目「サーバとホスト」では、ホストの概要、運用、設定に関するインタビュー質問が実行される。このインタビュー質問の回答から、ホストの脆弱性、ホストとサーバに関するコーポレートレベルポリシー等が導かれる。

【０１６７】

サーバとホスト含まれる質問群は、多くはコーポレートレベルポリシーに影響を与える質問であるが、プロダクトレベルポリシーに影響を与える質問もある。

【０１６８】

項目「サーバとホスト」には、さらに小項目として、以下の項目が含まれている。

【０１６９】

３．１　サーバとホストプロパティ

３．２　認証と識別

３．３　監査とログ

３．４　アクセス制御

３．５　変更手続き

３．６　災害復旧とバックアップ

３．７　オペレーションの信頼性

３．８　物理的セキュリティ

（４）アプリケーションとデータベース

項目「アプリケーションとデータベース」では、アプリケーションの概要、運用、設定に関するインタビュー質問が実行される。このインタビュー質問の回答から、アプリケーションの脆弱性、アプリケーションに関するコーポレートレベ

ルポリシー等が導かれる。項目「アプリケーションとデータベース」に含まれる質問群は、多くはコーポレートレベルポリシーに影響を与える質問であるが、プロダクトレベルポリシーに影響を与える質問もある。

【０１７０】

項目「アプリケーションとデータベース」には、さらに小項目として、以下の項目が含まれている。

【０１７１】

４．１　アプリケーション、データベースのプロパティ

４．２　認証と識別

４．３　監査とログ

４．４　アクセス制御

４．５　変更手続き

４．６　災害復旧とバックアップ

４．７　オペレーションの信頼性

４．８　物理的セキュリティ

（５）重要性の高いセキュリティ項目

項目「重要性の高いセキュリティ項目」では、一般的にファイアーウォールを構築する際に必要な情報に関するインタビュー質問が実行される。このインタビュー質問の回答から、コーポレートレベルポリシー、プロダクトレベルポリシー等が導かれる。項目「重要性の高いセキュリティ項目」に含まれる質問群の多くはコーポレートレベルポリシーやプロダクトレベルポリシーに関する質問であるが、エグゼクティブレベルポリシーに影響を与える質問もある。

【０１７２】

項目「重要性の高いセキュリティ項目」には、さらに小項目として、以下の項目が含まれている。

【０１７３】

５．１　ファイアーウォールの管理

５．２　パケットフィルタリング

５．３　ＮＡＴ（ネットワークアドレス変換）

５．４　ＳＭＴＰコンテンツフィルタリング

５．５　ＦＴＰコンテンツフィルタリング

５．６　ＨＴＴＰコンテンツフィルタリング

５．７　ログとアラート

（６）補正項目

項目「補正項目」では、一般的にＶＰＮを構築する際に必要な情報に関するインタビュー質問が実行される。このインタビュー質問の回答から、コーポレートレベルポリシー、プロダクトレベルポリシー等が導かれる。

【０１７４】

項目「補正項目」には、さらに小項目として、以下の項目が含まれている。

【０１７５】

６．１　ＶＰＮのプロパティ

６．２　ＶＰＮの管理

６．３　鍵の配布

６．４　ログと監査

Ｂ－２　インタビューの形式

インタビューの内容は、上記各項目の通りであるが、インタビューは、記述式や、選択式等種々の形式でなされる。

【０１７６】

Ｂ－３　インタビューの対象者

本実施の形態のセキュリティポリシードラフト構築装置２０は、インタビューの対象となるメンバーによって、質問の内容を変更する。換言すれば、被インタビュー者の職務内容に基づいて、質問の内容を制御しているのである。

【０１７７】

その結果、被インタビュー者に対して行うべき適切な質問を生成することが可能である。

【０１７８】

メンバーの職務内容によって決定されるのは、質問群のいわばコースである。各コースにおいて出される質問は、メンバーの回答内容によって変更される。た

とえば、ＶＰＮを使用しているかという質問に対して、使用していないと回答すれば、ＶＰＮの詳細に関する質問はスキップされる。しかし、ＶＰＮを使用していると回答した場合には、その回答をしたメンバーには、ＶＰＮの詳細に関する質問がなされる。

【０１７９】

このような制御は、いわゆる知識ベースのエキスパートシステムを利用して実行される。

【０１８０】

そのため、実際のインタビューに先立って、被インタビュー者の職務内容をセキュリティポリシー構築装置２０に入力する必要がある。具体的には、以下の項目に関して入力を行う。

【０１８１】

＊名前

＊部署名

＊役職

郵便番号

住所

国名

電話番号

ＥＭＡＩＬアドレス

＊タイプ

これらの項目の中で、＊が頭に付されている項目は必須入力項目である。また、タイプとは、職務内容を表す記号であり、本実施の形態では、図６に示される記号を用いて職務内容を表している。簡単に言えば、このタイプはいわゆる職務内容を表す。このタイプに基づき、質問すべき内容が決定される。本実施の形態で取り扱うタイプの一覧表が図６に示されている。

【０１８２】

なお、実際に被質問者に質問される内容は、質問の回答によって変化する。これはいわゆる知識ベース（Knowledge Base）の動作となる。たとえば、パスワー

ドの有効期限は存在するか？という質問に対し、有効期限はなく無制限だと回答したメンバーに対して、有効期限は何日か？という質問は行わない。これに対して、有効期限はあると答えたメンバーに対しては、有効期限は何日か？という質問が出されうる。

【０１８３】

Ｂ－４　管理すべき情報資産

本実施の形態では、セキュリティを確保する情報資産を５種類に分類している。その５種類は、ネットワーク、ホスト、アプリケーション、ユーザグループ、その他である。本実施の形態のセキュリティポリシー構築装置に情報資産を入力する場合には、以下の４項目を入力する。ただし、「ホスト」「ネットワーク」に属するアセットの場合は、さらに２項目、「ＩＰアドレス」「サブネットマスク」を入力する。

【０１８４】

アセット（資産）ＩＤ

＊アセットタイプ

＊アセット名

詳細

このうち、アセットタイプには５種類のタイプがある。

【０１８５】

Ａ　アプリケーション

Ｈ　ホスト

Ｎ　ネットワーク

Ｕ　ユーザグループ

Ｗ　その他、ＵＲＬ、ドメイン名、ファイル名

ここで、ユーザグループとは、共通の特徴を有するユーザの論理的な集合をいう。たとえば、会計情報を取り扱い、会計情報を修正、分析、報告するユーザを会計グループと呼ぶ。ユーザグループは１人または２人以上のユーザから構成される。なお、ユーザとは、その情報資産を使用する人間をいう。

【０１８６】

Ｂ－５　セキュリティポリシードラフトの作成

以上のような質問に対する回答をセキュリティポリシードラフト構築装置２０に入力することによって、セキュリティポリシーの構築が実行される。この装置は、いわゆるエキスパートシステムであり、生成した質問に対する回答を入力することによって、セキュリティポリシーを生成し、出力する装置である。このように質問に対する回答を入力することによって何らかのデータを生成する装置は、従来からエキスパートシステムとしてよく知られているため、その詳細は省略する。

【０１８７】

本実施の形態においては、エグゼクティブレベルポリシー、コーポレートレベルポリシー、プロダクトレベルポリシーの３種類のセキュリティポリシーが生成される。したがって、セキュリティポリシーのドラフトに関しても、これら３種類のドラフトが作成される。

【０１８８】

（１）エグゼクティブレベルポリシー

エグゼクティブレベルポリシーは、団体のセキュリティに関する「考え方」「方針」を記述したものである。

【０１８９】

エグゼクティブレベルポリシーには、たとえば以下の項目が含まれる。

【０１９０】

アクセス制御

情報資産に対するアクセス権の管理及び制御は、その情報資産の所有者が制御する必要がある。また、制御は、情報資産が保存又は処理される制御システムが有するアクセス制御の仕組みを使用しなければならない。このアクセス制御では、アクセス権の制御に関するその団体の考え方、方針を記述する。

【０１９１】

情報正確性

情報の内容を維持することは極めて重要な事項である。たとえば、情報は業務上の決定に必要不可欠なものだからである。この情報正確性においては、情報の

内容の正確性に関する団体の考え方、方針が記述される。

【０１９２】

保証

団体は、情報リソースや、セキュリティ対策の適切な安全性を保証するために適切な措置を採用しなければならない。この保証では、そのような措置に関する団体の方針、考え方を記述する。

【０１９３】

アカウンタビリティ

すべてのシステムはユーザのアクティビティを記録し、分析を可能にしなければならない。各ユーザは、自己の行為に責任を持たなければならない。このアカウンタビリティにおいては、各ユーザの自己の責任に関する団体の考え方、方針を記述する。

【０１９４】

識別・認証

すべてのユーザは、情報の機密性に応じて、適切に識別されなければならない。この識別・認証では、このような識別に関する団体の考え方、方針を記述する。

【０１９５】

緊急時対応計画

団体はシステムやネットワークにおける妨害に対する適切な対処を保証するために、詳細な計画と手続を作成しなければならない。この可用性においては、このような計画と手続に関する団体の考え方、方針を記述する。

【０１９６】

セキュリティ認識

従業員及び経営陣は、団体の情報セキュリティの要件を認識すると同時に自己の責任を自覚しなければならない。このセキュリティ認識においては、このような自己の責任に関する団体の考え方、方針を記述する。

【０１９７】

情報分類

情報セキュリティは、情報資産を保護するためのものである。したがって、保護すべき対象である情報資産は分類され、各分類にしたがって適切に保護されなければならない。情報分類では、この情報資産に関する団体の考え方、方針を記述する。

【０１９８】

職業倫理

ユーザは、道徳心を持って情報を取り扱わなければならない。ユーザはその行為を道徳心を持たずに情報を取り扱った場合には、処罰の対象となる。ユーザは処罰の対象となることを認識しなければならない。職業倫理では、ユーザの道徳心についての団体の考え方、方針を記述する。

【０１９９】

文書管理

セキュリティの仕組みはすべて適切に文書化しなければならない。文書管理では、この文書化に関する団体の考え方、方針を記述する。

【０２００】

調査

団体はセキュリティポリシー侵害が発生した場合には、その侵害を調査し、その侵害の内容をすべて文書化しなければならない。調査では、このようなセキュリティポリシー侵害に関する調査や文書化についての団体の考え方、方針を記述する。

【０２０１】

プライバシー

情報の使用は関係当事者のプライバシーを保証することを前提としなければならない。プライバシーでは、このプライバシーの保証に関する団体の考え方、方針を記述する。

【０２０２】

リスク管理

情報の所有者は、潜在するリスクを評価し、適切な制御、または防衛策を講じなければならない。リスク管理では、このような評価、制御、防衛策に関する団

体の考え方、方針を記述する。

【０２０３】

検証

団体は、すべてのセキュリティの実装を定期的に検証しなければならない。検証では、このような検証に関する団体の考え方、方針を記述する。

【０２０４】

資産評価

団体は情報資産を分析しなければならない。資産評価では、この分析に関する団体の考え方、方針を記述する。

【０２０５】

（２）コーポレートレベルポリシー

コーポレートレベルポリシーは、団体の情報資産に対してエグゼクティブレベルポリシーの記述を適用し、セキュリティの「運用規定」を記述したものである。この適用は、団体の運用ユニット毎に行われる。運用ユニットとは、情報システムを構成する部分をその作用に基づいてグループ分けしたものである。たとえば、ネットワークや、ホスト、アプリケーション等が、それぞれ運用ユニットである。

【０２０６】

エグゼクティブレベルポリシーはいわば「憲法（大原則）」を記述したものであるのに対し、コーポレートレベルポリシーは「法律（大原則に基づく規定）」を記述したものである。

【０２０７】

コーポレートレベルポリシーには、トップレベルとサブレベルの２レベルがある。

【０２０８】

トップレベル

トップレベルは、団体に存在する運用ユニット全体に関するポリシーである。たとえば、各運用ユニット毎にそれに対する規定が記述される。

【０２０９】

ネットワーク

このネットワークには、団体ネットワークの全体に対する規定が記述される。

【０２１０】

ホスト

このホストには、団体ホストの全体に対する規定が記述される。

【０２１１】

アプリケーション

このアプリケーションには、団体アプリケーションの全体に対する規定が記述される。

【０２１２】

サブレベル

さて、サブレベルは、運用ユニットをより細分化した個々のユニットに関する特定のポリシーが記述される。たとえば、以下のような項目が記述される。

【０２１３】

ソフトウェア管理

このソフトウェア管理には、その団体内で用いられる個々のソフトウェアに関するそのソフトウェアの使用やライセンス管理の規定が記述される。

【０２１４】

ダイヤルアップ

このダイヤルアップには、その団体内で用いられる個々のリモートアクセスサーバに関する規定が記述される。

【０２１５】

電子メール

この電子メールには、その団体内で用いられる個々の電子メールの規定が記述される。

【０２１６】

ファイアーウォール管理

このファイルウォールには、その団体内で用いられる個々のファイアーウォールの管理の規定が記述される。

【０２１７】

暗号

この暗号には、その団体内で用いられる個々の暗号化の実装規定が記述される。

【０２１８】

電子商取引

この電子商取引には、その団体内で用いられる個々の電子商取引の規定が記述される。

【０２１９】

ネットワーク

このネットワークには、その団体内で用いられる個々のネットワークの規定が記述される。

【０２２０】

ホスト

このホストには、その団体内で用いられる個々のホストの規定が記述される。

【０２２１】

アプリケーション

このアプリケーションには、その団体内で用いられる個々のアプリケーションの規定が記述される。

【０２２２】

なお、トップレベルのコーポレートレベルポリシーは、情報役員や管理職に対するインタビューで収集した情報（すなわち回答から判明した情報）に基づき作成される。トップレベルのコーポレートレベルポリシーを作成するのには、システム管理者に対するインタビューを実施しなくても良い。ここで、システム管理者とは、ネットワークセグメント、ホスト、またはアプリケーションのシステム管理者を言う。

【０２２３】

一方、サブレベルのコーポレートレベルポリシーは、システム管理者に対するインタビューの結果が必要となる。もちろん、このためには、システムレベルの

インタビューを行う必要がある。システムレベルのインタビューとは、システム管理者に対し、個別の運用ユニットに関する質問を行うインタビューである。

【０２２４】

（３）プロダクトレベルポリシー

プロダクトレベルポリシーは、情報資産をどのようなリソース（セキュリティ商品、運用体制）及びその設定を使って保護するか、具体的な「方法」を記述したものである。上記エグゼクティブレベルポリシーやコーポレートレベルポリシーが、方針や管理面におけるルールを記述しているのに対して、プロダクトレベルポリシーは、ハードウェアやソフトウェアの細部にまで言及し、エグゼクティブレベルポリシーが提供する「原則」と、コーポレートレベルポリシーが提供する「規定」とに基づいて、具体的にどのように情報資産の保護を実現するかに関する「方法」を提供するものである。したがって、プロダクトレベルポリシーは、具体的な技術の実装に関する記述を含むものである。

【０２２５】

このプロダクトレベルポリシーは、ソフトウェアやハードウェアに関する記述を含み、さらに、それらを具体的に運用するルールも記述されている。

【０２２６】

ただし、プロダクトレベルポリシーは、遵守すべきルールという性格は希薄である。実際の業務遂行上の理由で、使用する製品が変更される場合もあるかもしれないし、また、機器の故障で代替機器を使用する場合もあるかもしれない。これらの状況に対する責任や製品の基準は、上記エグゼクティブレベルポリシーやコーポレートレベルポリシーが規定する「原則」や「規定」に委ねられている。換言すれば、これらの状況に対する対策等は上記エグゼクティブレベルポリシーやコーポレートレベルポリシーで十分に規定される必要がある。

【０２２７】

さて、上述したエグゼクティブレベルポリシーは、いわば原則を謳ったものであり、たとえば、「アクセス権は、業務終了と共に抹消されなければならない。」

の如きルールである。

【０２２８】

また、コーポレートレベルポリシーは、具体的な規定を謳ったものであり、たとえば、「アクセス権はＯＳで制御されなければならない。」の如きルールである。

【０２２９】

これに対して、プロダクトレベルポリシーは、具体的な手段を規定するものであり、たとえば、「サーバＡのアクセス権の制御は、管理者Ｘによって管理される。業務上の必要がある者は、管理者Ｘに依頼し、アクセス権を得る。業務終了後は速やかに管理者Ｘに依頼し、アクセス権を抹消する。」の如き記述である。

【０２３０】

さらに、本実施の形態では、プロダクトレベルポリシーとして、２レベルのプロダクトレベルポリシーを作成する。

【０２３１】

第１レベルは、エグゼクティブレベルポリシーやコーポレートレベルポリシー等と同様に、自然言語で記述されたものであり、上で述べた例もこの第１レベルのプロダクトレベルポリシーである。

【０２３２】

第２レベルは、具体的な装置の設定を記述したスクリプトである。すなわち、各機器（ハードウェアだけでなくソフトウェアも含む）の設定スクリプトそのものを記述したものであり、そのまま、各機器の設定に用いることができるものである。本実施の形態では、プロダクトレベルポリシーとして各装置の具体的なスクリプトを作成しているため、実際にファイアーウォールやルータなどの装置の設定を行う際の労力が軽減できるという効果がある。

【０２３３】

Ｃ．ステップ３：システム及びその運用の実査・分析

このステップでは、構築したセキュリティポリシーのドラフトと、実際の情報システム及びその運用手法との差異を検査し、分析を行う。この分析は、差異を見つけだすことに加え、さらに、その対策案を優先度と共に示すために行う。

【０２３４】

このステップの実査の分析は以下の２レベルからなる。

【０２３５】

Ｃ－１　レベル１の実査と分析

セキュリティポリシーのドラフトは、質問とその回答により作成されている。このプロセスにおいては、回答にばらつきや矛盾が生じる可能性がある。また、回答が正しいとは限らない。

【０２３６】

そこで、レベル１の実査と分析では以下のことを実行する。

【０２３７】

まず、複数の回答に矛盾があるか否か調査する。さらに、セキュリティポリシーのドラフトと、インタビューの回答から想定される情報システムとの比較を行う。そして、セキュリティポリシーのドラフトと、実際の情報システムの実査を行ってプルーフを行った情報システムとの比較を行って、その差異を検出する。

【０２３８】

実際の調査は、エキスパートシステムである分析装置を用いて実行する。この分析装置３０の構成ブロック図が図７に示されている。この図に示すように、分析装置３０は、回答群に互いに矛盾する回答があるか否か検査する矛盾検査手段３２を備えている。この検査結果は、矛盾出力手段４０に供給される。

【０２３９】

矛盾出力手段４０は、検査結果を、インタビュー結果矛盾レポートとして外部に出力する。

【０２４０】

インタビュー結果矛盾レポートの内容は、整合手段４１に供給される。整合手段４１は、回答間に矛盾があった場合の処理を実行する。この処理は２種類あり、利用者がいずれかを選択することが可能である。

【０２４１】

（１）各メンバーの職務内容に基づいて、知識ベースを利用して、最も確からしい回答を採用する。

【０２４２】

（２）矛盾点に関し、再インタビューを実施する。または実際に調査を行って情報システムの実態を知る。再インタビューと実際の調査との双方を実施することも好ましい。を

このようにして整合をとったインタビューの結果（すなわち回答）は、仮想構築手段３４に供給される。

【０２４３】

仮想構築手段３４は、整合がとれた回答群に基づき、その団体の情報システムを仮想的に構築する。さて、このようにして仮想構築手段３４が構築した情報システムの構成や運用は差異出力手段３８に供給される。

【０２４４】

また、分析装置３０は、その団体の実際の情報システムの構成や運用を入力する実システム入力手段３６を備えている。この実システム入力手段３６が入力した実システムの構成や運用は、上記差異出力手段３８に供給される。

【０２４５】

さらに、差異出力手段３８には、セキュリティポリシーのドラフトが供給される。このような構成の下、差異出力手段３８は、以下の２つの比較を実行し、それぞれ差異を検出・出力する。

【０２４６】

（１）セキュリティポリシーのドラフトと、インタビュー結果との差異分析。

【０２４７】

（２）セキュリティポリシーのドラフトと、インタビュー結果を実査によってプルーフをとったものとの差異分析。

この（１）の差異分析においては、セキュリティポリシーのドラフトと、仮想構築手段３４が構築した情報システムとの比較が実行される。この両者は、基本的には、メンバーへのインタビューの結果（回答）に基づき、構築されているため、ほとんど差はないとも考えられる。しかしながら、セキュリティポリシーは、セキュリティポリシーといえるためには、最低限度の要件が必要である。

【０２４８】

たとえば、インタビューの回答が「パスワードが無制限に有効」である場合も

、セキュリティポリシーにおいて、パスワードが無制限に有効とすることはできない。パスワードに期限があることはセキュリティポリシーの基本的な要件であり、これなくしてセキュリティポリシーとは言えない。

【０２４９】

したがって、セキュリティポリシーのドラフトと、上記インタビュー結果の差異は存在するのである。この検出した差異は、分析レポートとして出力される。

【０２５０】

この分析レポートによって、インタビューの結果がセキュリティポリシーの観点から修正すべき点を見つけることができる。

【０２５１】

また（２）の差異分析においては、セキュリティポリシーのドラフトと、上記構築した仮想的な情報システムを実査によってプルーフしたものと、の比較が実行される。

【０２５２】

上述したように、仮想的な情報システムはインタビューによってのみ構築されている。したがって、実システムとは異なっている可能性がある。そのため、実査によって、この仮想的な情報システムを実際の情報システムでプルーフしたものと、セキュリティポリシーのドラフトとの比較をすれば、一層正確に現在の実システムの修正すべき点を知ることができる。

【０２５３】

このプルーフをするための実査は、精密にすればするほど好ましい。しかし、情報システムのすべてを実査するのは、大きな労力とコストが必要である。さらに、インタビューをした意味が希薄になってしまう。

【０２５４】

そこで、一般には、インタビューの回答を補助できる程度の実査を行い、上記仮想的情報システムのプルーフをし、プルーフをした情報システムとセキュリティポリシーの差異分析を行うのが、効率的である。

【０２５５】

たとえば、インタビューの回答に矛盾がある部分を重点的に実査することも好

ましい。さらに、被質問者であるメンバーが忘れてしまった等の理由により回答できない部分を重点的に実査することも好ましい。

【０２５６】

どの程度、実査を行うかは、要求される精度、期限、コストなどによって決定すべきである。このようにして、求めた差異は、分析レポートとして出力される。

【０２５７】

なお、これら（１）及び（２）の比較は、いずれか一方のみを行っても良いし、双方を実行してもかまわない。まず、（１）の比較を実行し、不十分であると判断する場合には、さらに（２）を実行することも好ましい。

【０２５８】

また、後述するレベル２の実査と分析で得られた優先度を考慮し、優先度の高い部分を実査の対象とすることも好ましい。

【０２５９】

次に、図８には、本ステップ３の動作を表すフローチャートが示されている。このフローチャートは上記図１のステップＳ１－３をより詳細に表したものである。

【０２６０】

ステップＳ８－１においては、矛盾検査手段３２を用いて、回答群中に矛盾のある回答があるか否か検査する。また、ステップＳ８－２においては、差異出力手段３８を用いて、セキュリティポリシーのドラフトと、インタビュー結果との間に差異があるか否か検査する。ここで、インタビュー結果とは、インタビューの回答によって構築した仮想情報システムと、この仮想情報システムを実査によってプルーフしたシステム、の２種類を含む。

【０２６１】

なお、ステップＳ８－１とステップＳ８－２とは特に順番は存在しない。ステップＳ８－２を先に実行してもかまわない。

【０２６２】

このように、本実施の形態によれば、図７に示すような分析装置３０を用いて

いるため、回答群に含まれる回答の間に矛盾があるか否か、回答の内容と実システムとの間に差異があるか否か、を迅速に知ることができる。

【０２６３】

なお、分析装置３０は、いわゆるエキスパートシステムであり、上記各手段は、コンピュータ上で動作するソフトウェアで実現することが望ましい。

【０２６４】

Ｃ－２　レベル２の実査と分析

このレベル２の実査と分析では、上記レベル１で得た差異を、人的体制の差異、運用方法の差異、技術的対策の差異、の３種類に分類する。そして、各差異毎に、その対策と優先度を検討する。

【０２６５】

以下、ネットワークポリシーについて差異がある場合の対策と優先度の例を示す。

【０２６６】

（１）差異１

種類　：人的体制の差異

内容　：ネットワークポリシーでは、ネットワークセグメントの管理者を明らかにする、となっているが、実システムでは明らかではない。

対策　：管理者または所有者を明確に割り当てる。

【０２６７】

優先度：即刻

（２）差異２

種類　：技術的対策の差異

内容　：ネットワークポリシーでは、ネットワークのユーザ認証で使用するパスワードは長期間使用していなければ抹消されると規定されている。しかし、実システムでは抹消する仕組みがない。

対策　：３０日間使用しないユーザアカウントがあればそのパスワードを抹消する仕組みを設ける。

【０２６８】

優先度：高い

図８のフローチャートにおいては、ステップＳ８－３が、上記対策とその優先度を求める動作に相当する。

【０２６９】

このように、本実施の形態によれば、回答群と、実システムとの差異を解消するための対策が立てやすくなるため、セキュリティポリシーと実システムとの間の不一致をなくすことが容易となる。

【０２７０】

Ｄ　ステップ４：ポリシー調整・ルール調整

さて、上記ステップ３によって、実システムとセキュリティポリシードラフトとの間の不一致点が明確になり、またそれに対する対策と優先度が明らかになった。本ステップ４では、対策の検討と、実際の作業を実行する。

【０２７１】

対策は、大きく２種類に分かれる。

【０２７２】

（１）セキュリティポリシードラフトに調整を加えて実システムに合わせる。

（２）実システム側の運用ルール等を調整する。

【０２７３】

以下、これらを詳細に説明する。

【０２７４】

Ｄ－１　セキュリティポリシードラフトの調整

セキュリティポリシーのドラフトは、既に説明したようにグローバルガイドラインと呼ばれる、標準的なセキュリティポリシーを構築するための基本的な項目、内容を、適宜組み合わせて構築している。現在、有名なグローバルガイドラインは数種類知られており、本実施の形態では、その数種の中から適宜ルールや方針等を取り出して組み合わせてセキュリティポリシーの構築を行っている。ドラフトの段階では、これら数種のグローバルガイドライン中最も条件の厳しいものを選び出し、セキュリティポリシーのドラフトに組み込んでいる。

【０２７５】

換言すれば、これらグローバルガイドラインは、その種類によって各規定の強度が異なっているのである。たとえば、あるグローバルガイドラインでは、パスワードの有効期限を６０日としているが、他のグローバルガイドラインではこれを１８０日と規定している。

【０２７６】

すなわち、ドラフトの段階では、最も厳しい条件で各ルール等が構築されているのである。したがって、団体側の意向によっては、セキュリティポリシーのドラフト内の各ルールの強度が強すぎると判断される場合もあろう。このような場合には、適宜弱いルールに変更することが好ましい。

【０２７７】

たとえば、同一のパスワードの有効期限を６０日とするルールが厳しい、すなわち強いルールである場合には、団体側との話し合いによって有効期限を１８０日に変更する、すなわち弱いルールに変更するのである。

【０２７８】

このように、各団体の意向に基づき、ルールの強度を変更すれば、実システムと合致したセキュリティポリシーを構築することが可能である。

【０２７９】

このようにして、セキュリティポリシーのドラフトの調整が実行される。

【０２８０】

Ｄ－２　ルール調整

上述したレベル２の実査と分析において説明した対策に基づき、実システム側の運用を調整する。このルール調整は、運用方法を変更するものや、さらに、セキュリティシステム（たとえばファイアーウォール）のルール設定の修正等がある。

【０２８１】

Ｅ　ステップ５：プライオリティプランニング

上記ステップ４までで、団体の実際の情報システムに関するセキュリティポリシーの構築が完了する。

【０２８２】

しかし、今後、このセキュリティポリシーに合わせてセキュリティ対策を順次実行していく必要がある。そこで、本ステップ５では、優先順位を含めて各種対策を検討し、リストにしておく。このようなリストを作成しておくことで、今後のセキュリティ対策の計画を立てることができる。さらには、その計画に基づき、予算の検討を行うことができる。すなわち、情報セキュリティ対策の予算化を実現することができるのである。このようなリストがなければ、将来の情報セキュリティ費用がどの程度かかるのか見通しが立てたず、予算化が困難になることも考えられる。

【０２８３】

セキュリティ対策には、セキュリティシステムの導入及びテストの他に、セキュリティポリシーを遵守するための従業員の教育、システムログの分析、等の作業も含まれる。

【０２８４】

また、セキュリティポリシーには、ネットワーク監視と、セキュリティポリシーに基づく運用の監査と、セキュリティポリシーの見直しと、が含まれる。

【０２８５】

なお、団体側の情報システムの変更、運用の変更等に合わせて、セキュリティポリシーも変更をする必要がある。そこで、定期的にセキュリティポリシーの見直しを行う必要がある。

【０２８６】

Ｆ　ステップ６：セキュリティ強化策実行

上記ステップ５において作成した優先順位を含めたセキュリティ対策リストに基づき、実際にセキュリティ強化策を実行していく。この実行は上記リスト及びセキュリティポリシーに従ったものであり、円滑に作業を進めることが可能である。

【０２８７】

以上述べたように、本実施の形態では、セキュリティポリシーの構築からメンテナンスまでを６ステップに分けて実行している。したがって、セキュリティポ

リシーを段階的に構築、実行していくことが可能であり、団体側の要望に合った作業の進め方を実現可能である。

【０２８８】

【発明の効果】

以上述べたように、本発明によれば、団体のメンバーに質問をすることによって、その回答に基づき、セキュリティポリシーを構築している。従って、セキュリティポリシーを容易に構築することができる。

【０２８９】

さらに、本発明によれば、段階的にセキュリティポリシーの構築を行っているため、団体の要望（予算など）に応じた柔軟な構築方法を実行することが可能である。

【０２９０】

また、本発明によれば、団体の情報セキュリティの状況を診断するので、団体は情報セキュリティの重要性を知ることができる。

【０２９１】

また、本発明によれば、セキュリティ対策を優先度と共に知ることができるため、将来の情報セキュリティ対策の計画を立案しやすくなる。さらに、この計画に基づき、団体の予算の検討を行うことが可能となる。

【図面の簡単な説明】

【図１】

本発明の好適な実施の形態のビジネスモデルの原理を表すフローチャートが示されている。

【図２】

評価装置の構成ブロック図である。

【図３】

評価書の作成作業の動作を表すフローチャートである。

【図４】

セキュリティポリシードラフト構築装置の構成ブロック図である。

【図５】

セキュリティポリシードラフト構築装置を用いてセキュリティポリシーのドラフトを構築する動作を表すフローチャートである。

【図６】

職務内容を表すタイプの一覧表を示す図である。

【図７】

分析装置の構成ブロック図である。

【図８】

システム運用　実査・分析の動作を表すフローチャートである。

【符号の説明】

１０　評価装置

１２　質問生成手段

１４　記憶手段

１６　回答保管手段

１８　セキュリティ完成度作成手段

２０　セキュリティポリシードラフト構築装置

２２　質問生成手段

２４　記憶手段

２６　回答保管手段

２８　ドラフト構築手段

３０　分析装置

３２　矛盾検査手段

３４　仮想構築手段

３６　実システム入力手段

３８　差異出力手段

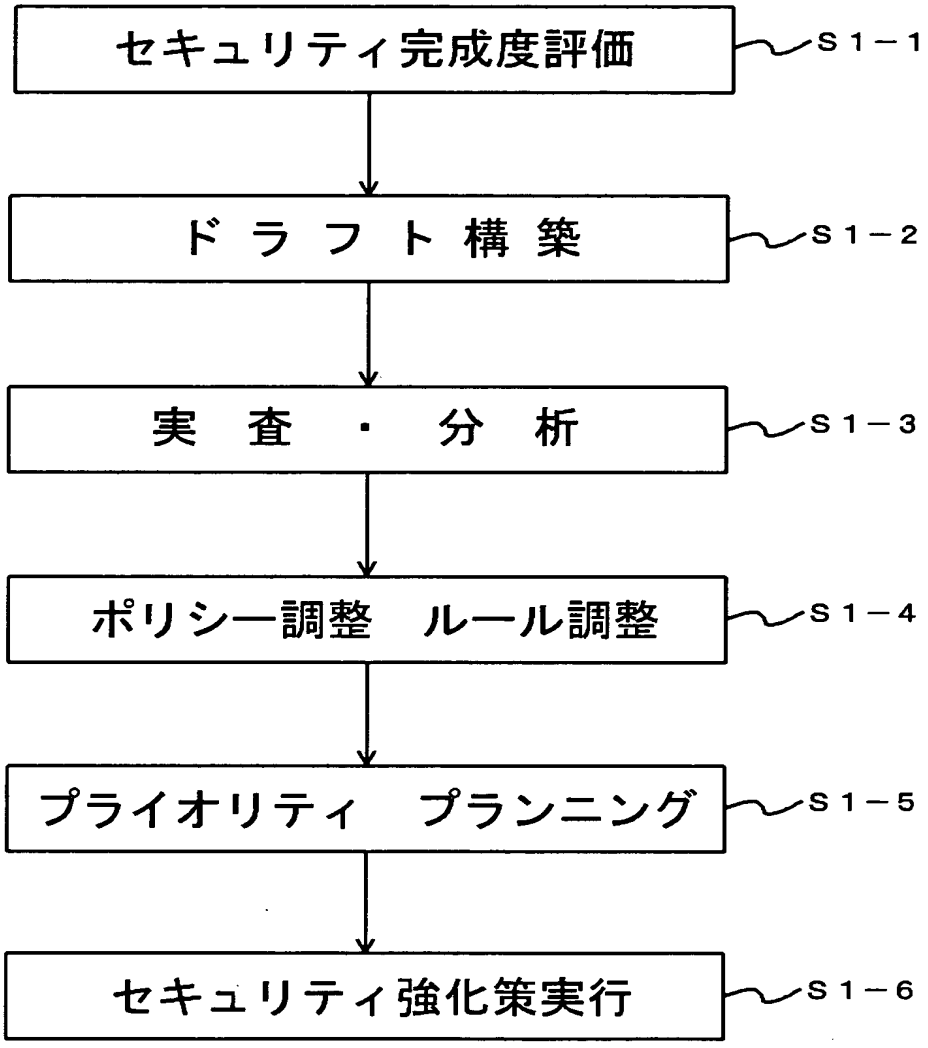
４０　矛盾出力手段

４１　整合手段

【書類名】　図面

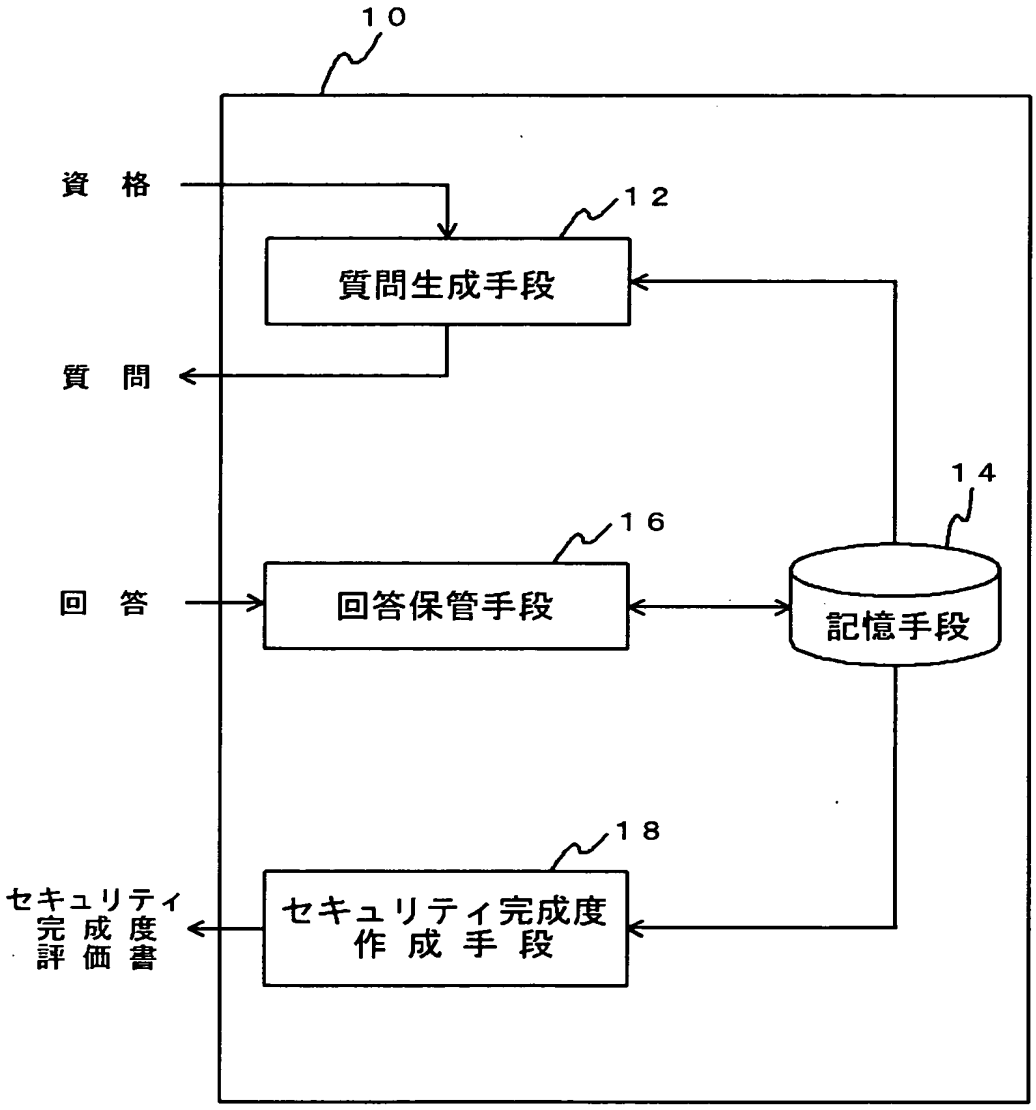
【図１】

図１　ＡＳＧ－０００１



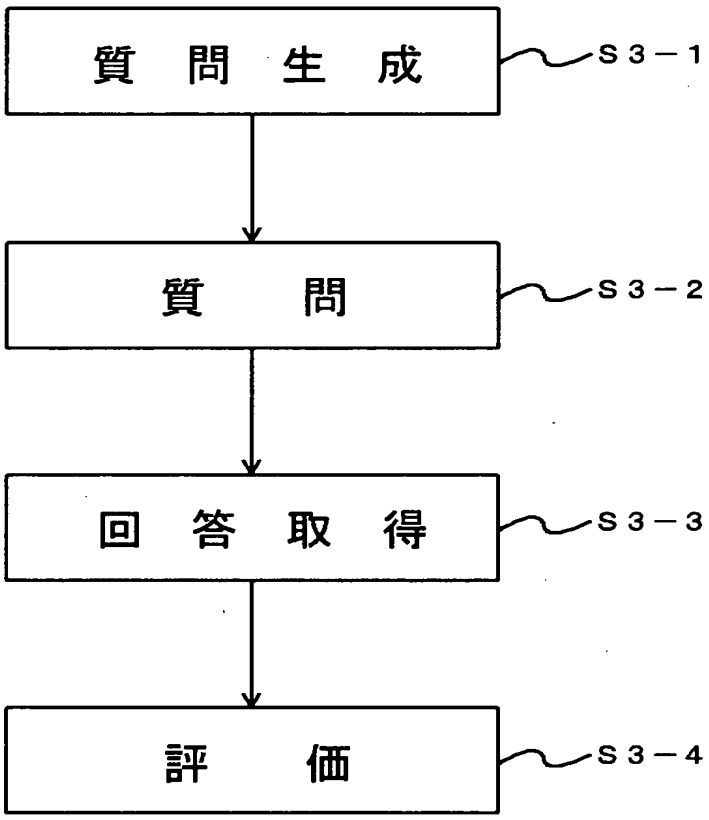
【図２】

図２　　ＡＳＧ－０００１



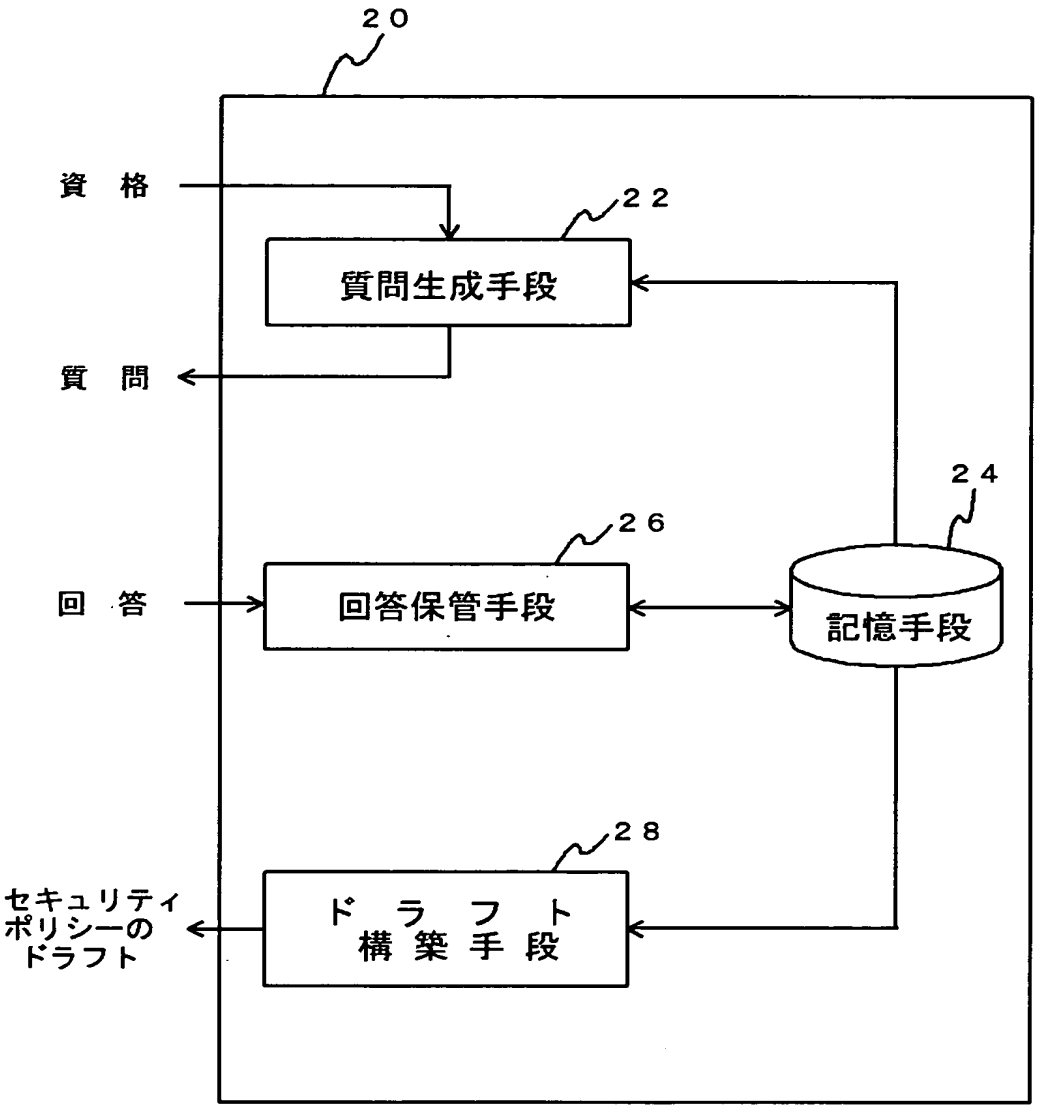
【図３】

図3　　ＡＳＧ－０００１



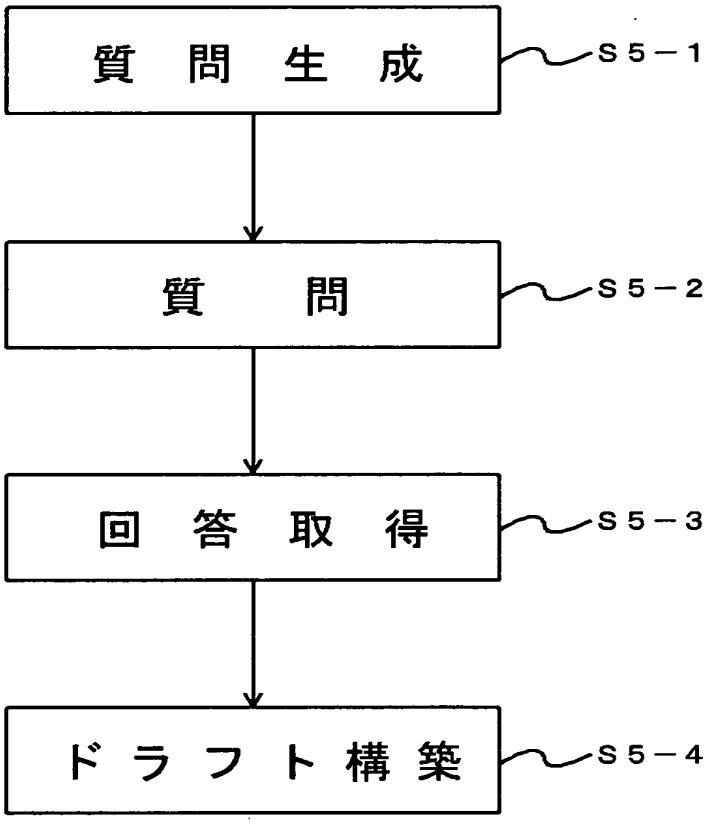
【図４】

図４　　ＡＳＧ－０００１



【図５】

図５　　ＡＳＧ－０００１



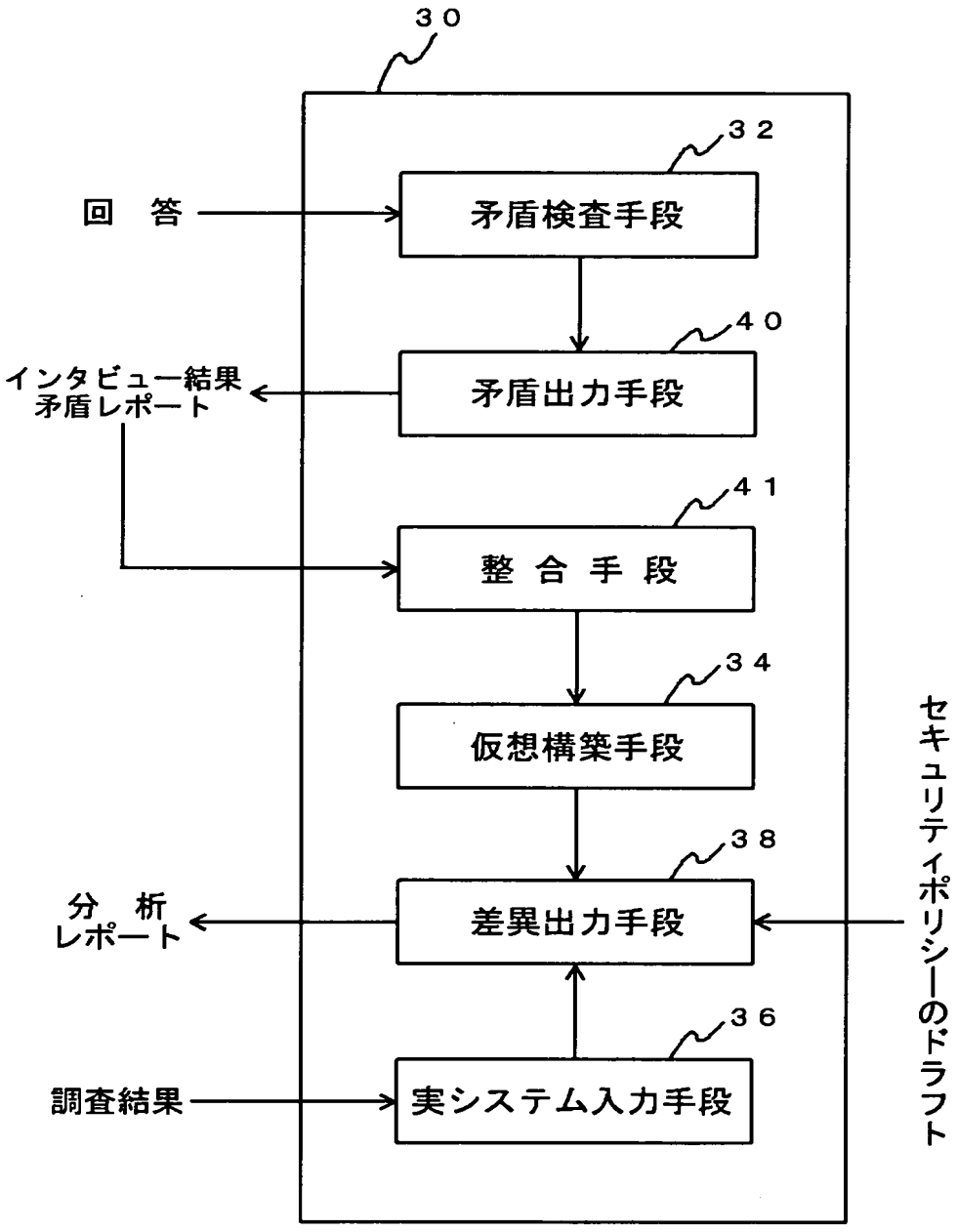
【図６】

図６　　ＡＳＧ－０００１

タイプ	定義
アプリケーション管理者 [APP]	アプリケーション、またはアプリケーションのグループの運用管理者
アプリケーションセキュリティ管理者 [ASA]	アプリケーション、またはアプリケーションのグループのローカルセキュリティ運用管理者
内部監査役員 [AUD]	内部監査を担当する役員
社長／最高経営責任者 [CEO]	社内の業務、運営、またはその他全般に関わる最終決定権を持つ役員 、または社長。
情報統括役員 [CIO]	情報統括役員。単なるコンピュータ担当者とは違い、企業戦略として情報システムの活用方法を立案、実行する情報資源管理の責任を持つ。情報、通信部門の最高責任者でもある。
災害復旧統轄役員 [DDR]	災害復旧を担当する上級役員
ダイヤルイン管理者 [DIA]	ネットワークセグメント、または部門のダイヤルイン担当の管理者
情報保護役員 [DIP]	情報セキュリティ担当の役員
災害復旧管理者 [DRA]	ネットワークセグメント、ホスト、またはアプリケーションの災害復旧管理者
部門セキュリティ管理者 [DSA]	ローカルのネットワークセグメント、ホスト、またはアプリケーションについての各部のセキュリティ管理者
通信担当役員 [DTC]	電話回線、広範囲なネットワーク接続を含む電気通信を担当する役員
Facilitator [FAC]	インタビュー実施者
ファイアウォール管理者 [FWA]	ファイアウォールのホストシステムの運用管理者
人事 [HR]	従業員の採用、教育を担当する部門
ホスト管理者 [HST]	ローカルホスト、またはローカルホストのグループの運用管理者
法律担当役員 [LEG]	法律顧問
ネットワークセグメント [Net]	ネットワークセグメント、またはネットワークセグメントのグループの運用管理者
ユーザデスクトップ管理者 [PCA]	ローカルユーザデスクトップコンピュータを担当する運用管理者

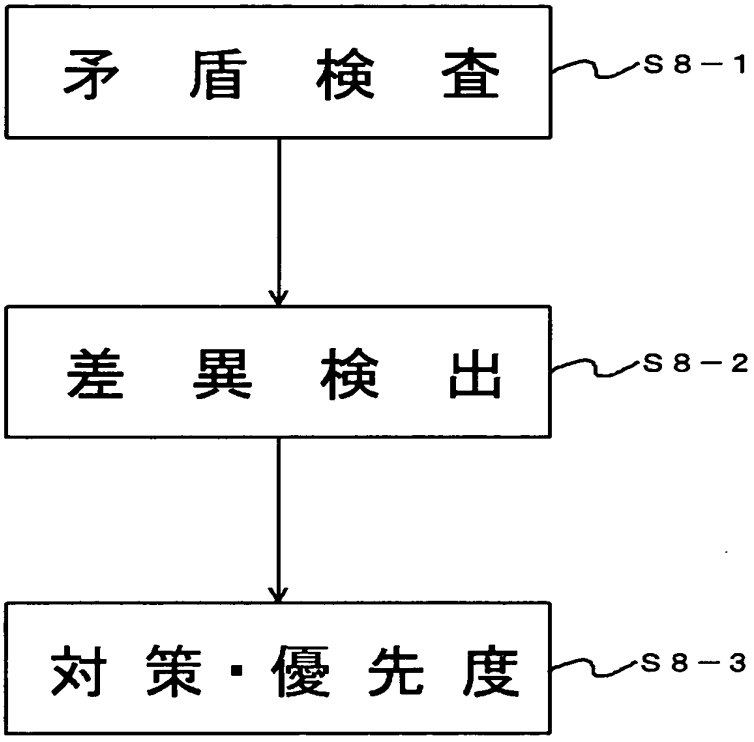
【図７】

図７　　ＡＳＧ－０００１



【図８】

図８　　ＡＳＧ－０００１



【書類名】　要約書

【要約】

【課題】　セキュリティポリシーを効率的に構築する方法及びセキュリティポリシーの構築を支援する装置を提供することである。

【解決手段】　６段階のステップからなるセキュリティ構築手法によれば、最初は簡易にセキュリティポリシーのドラフトを構築し、必要に応じ、団体の実態との再調整を行い、段階的に、セキュリティポリシーを完成していくので、各団体のスケジュールや予算に合わせてセキュリティポリシーを構築することが可能である。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２０００－１６４８１９
受付番号	５００００６８２５７８
書類名	特許願
担当官	風戸　勝利　　９０８３
作成日	平成１２年　６月　５日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】	500056448
【住所又は居所】	東京都中央区日本橋小網町１９－７
【氏名又は名称】	株式会社アズジェント

【代理人】　申請人

【識別番号】	100109014
【住所又は居所】	東京都新宿区四谷３丁目２番１７号　四谷中央ビル６Ｆ　伊藤国際特許事務所
【氏名又は名称】	伊藤　充

次頁無

出　願　人　履　歴　情　報

識別番号　　〔５００００５６４４８〕

１．変更年月日　　２０００年　２月１０日
［変更理由］　新規登録
住　所　東京都中央区日本橋小網町１９－７
氏　名　株式会社アズジェント